Enterprise Mobility Management

Benutzerhandbuch

Version R9

Deutsch

März 19, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2015 Kaseya. All rights reserved. | www.kaseya.com

Inhalt

Überblick 1
Enterprise Mobility Management Modulvoraussetzungen 2
Benutzeroberfläche 3
Konfigurieren der Active Directory Integration 4
Onboarding-Kunden 8
Onboarding von Benutzern 11
Verwalten von Geräten 12
    Befehlsstatus 13
    Audit-Aktionen 14
    Nachverfolgungsaktionen 14
    Messaging-Aktionen 14
    Verloren/Gefunden-Aktionen 14
    Geräteaktionen 15
    Benachrichtigungsaktionen 15
    Gerätedetails anzeigen 15
Regeln konfigurieren 18
    Benutzerdefinierte MDM-Richtlinien 19
        Konfigurieren eines Web Clip-Profils 19
        Konfigurieren eines WiFi-Profils 20
        Konfigurieren eines E-Mail-Profils 20
    Benutzerdefinierte BYOD-Profile 21
    Benutzerdef. Anwendungsrichtlinien 23
    Voreingestellte Richtlinien (schreibgeschützt) 23
        Voreingestellte MDM-Profile (schreibgeschützt) 23
        Voreingestellte BYOD-Richtlinien (schreibgeschützt) 25
Verwalten von Anwendungen auf Geräten 26
    Konfigurieren des App-Katalogs 26
    Anzeigen des App-Bestands 27
WorkBrowser und WorkDocs 28
    Verwendung von WorkBrowser 28
    Verwenden von WorkDocs 28
Protokollierung der Modulaktivität 30
Inhaltsverzeichnis 31

Überblick

Enterprise Mobility Management ist ein neues Modul, das eine integrierte Lösung für Unternehmen zur Verwaltung von mobilen Geräten, Anwendungen und sicherem Zugriff auf Unternehmensdaten nach Richtlinien bietet. Dazu gehört die in der Branche schnellste Implementierung für das Onboarding von Kundenunternehmen und deren Benutzern. Mobile Geräte können sich im Besitz von Unternehmen oder im Besitz von Mitarbeitern befinden. Firmenbestände werden immer von persönlichen Daten isoliert. Daten werden bei Ausführung und im Ruhezustand mittels AES-256-Verschlüsselung gesichert.

Mit der einfachen, benutzerfreundlichen integrierten Benutzeroberfläche können Sie schnell folgende Aktionen ausführen:

- Integrieren Sie neue und bereits vorhandene Kundenunternehmen in **Enterprise Mobility Management** mithilfe eines Setup-Assistenten.
- Wenden Sie hohe, mittlere und niedrige Sicherheitsrichtlinien an, die Sie anpassen können.
- Verwenden Sie voreingestellte Konfigurationsprofile für jede Sicherheitsebene.
- Senden Sie Einladungen an Benutzer, damit diese ihre Geräte registrieren. Bei der Registrierung wird eine Kaseya Agent-Anwendung namens *MobileManage* auf ihren Geräten installiert.
- Verwalten Sie mehrere Geräte für jeden Benutzer.
- Fordern oder verbieten Sie die Installation von Anwendungen auf mobilen Geräten.
- Identifizieren Sie installierte Anwendungen auf mobilen Geräten.
- Prüfen Sie jedes mobile Gerät und liefern Sie eine detaillierte Inventarisierung von Betriebssystem, Gerätedaten, Plattform und Netzwerkeigenschaften.
- Aktivieren oder deaktivieren Sie die Nachverfolgung des Standorts von mobilen Geräten in Echtzeit und speichern Sie den Standortverlauf.
- Lösen Sie auf den Geräten einen Alarm aus, sodass Benutzer ihre verlorenen Geräte wiederfinden können.
  - Sperren und löschen Sie verlorene bzw. gestohlene Geräte und setzen Sie sie zurück.
  - Erhalten Sie eine Meldung, wenn ein verlorenes Gerät eincheckt oder die Richtlinien nicht mehr erfüllt.
  - Senden Sie Textnachrichten von **Enterprise Mobility Management** an mobile Geräte.
  - Bieten Sie Benutzern von mobilen Geräten sicheren Zugriff auf die internen Websites und Dokumente ihres Unternehmens mithilfe von zwei Container-Anwendungen.
    - ✓ Die Website-Browser-Anwendung heißt *WorkBrowser*. Sie können optional den Zugriff auf verknüpfte interne Websites mit *WorkBrowser* unter Verwendung von Proxy-URLs kontrollieren.
    - ✓ Die Dokument-Browser-Anwendung heißt *WorkDocs*. *WorkDocs* ermöglicht einem Benutzer, Dokumente zu bearbeiten und lokal zu speichern oder geänderte Dokumente in die internen Netzwerke Ihrer Unternehmen hochzuladen.

Lizenzierung

- Die Lizenzierung beruht auf der Anzahl der Benutzer, die von **Enterprise Mobility Management** verwaltet werden. Jeder lizenzierte Benutzer kann über eine unbegrenzte Anzahl von Geräten verfügen, die mit **Enterprise Mobility Management** verwaltet werden.

Vereinfachte Benutzeroberfläche

Die Benutzeroberfläche enthält eine einzelne Seite mit vier Registerkarten. Jede Registerkarte enthält Drilldown-Menüs für:

- Benutzer
- Geräte

- Anwendungen
- Richtlinien

Active Directory Integration

Enterprise Mobility Management verwendet die Active Directory-Instanz eines Kundenunternehmens, um die Benutzer zu identifizieren, die zur Registrierung ihrer mobilen Geräte eingeladen wurden. Sicherheitsrichtlinien in **Enterprise Mobility Management** werden auf ein Gerät basierend auf dessen Zuordnung zu einem Active Directory-Benutzer angewandt. **Enterprise Mobility Management** speichert keine Benutzer-Anmeldedaten, sondern wirkt nur als Relais für die Active Directory-Authentifizierung.

Unterstützte mobile Geräte

Enterprise Mobility Management unterstützt die folgenden mobilen Geräte:

- IOS-Version (7.0 und höher)
- Android-Version 4.0.3 und höher

Erstversion

Für diese Erstversion wird **Enterprise Mobility Management** nur in lokalen Umgebungen unterstützt. Bei einem Upgrade auf R9 in einer lokalen Umgebung wird Mobile Device Management entfernt und **Enterprise Mobility Management** hinzugefügt. Die Migration von Daten von Mobile Device Management zu **Enterprise Mobility Management** wird nicht unterstützt.

> **Hinweis: Enterprise Mobility Management** kann die für die VSA angegebene **externe IP-Adresse** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#248.htm)* nur zum Zeitpunkt der Installation der VSA oder bei einem Upgrade auf R9 verwenden. Eine Änderung der externen IP-Adresse der VSA nach der Installation oder dem Upgrade wird nicht durch das **Enterprise Mobility Management**-Modul unterstützt.

Enterprise Mobility Management Modulvoraussetzungen

Kaseya Server

- Das Enterprise Mobility Management R9-Modul erfordert lokale VSA R9. Mobile Device Managementwird bei einem Upgrade deinstalliert.

  > **Hinweis:** SaaS VSA-Umgebungen verwenden bei einem Upgrade auf R9 weiterhin Mobile Device Management.

- Für dieses Modul muss VSA Internetzugang haben und mit einem Zertifikat von einer bekannten Stelle SSL-aktiviert sein.
- Kundenunternehmen müssen über Active Directory verfügen, um Benutzer zu Enterprise Mobility Management hinzuzufügen.

Anforderungen für verwaltete mobile Geräte

- IOS-Version (7.0 und höher)
- Android-Version 4.0.3 und höher

Anforderungen für Active-Directory-Server

- Ermöglicht Zugriff von der VSA. Port 389 oder 636 sollten geöffnet sein. Wenn VSA nicht dasselbe Intranet wie eine Active Directory-Instanz nutzt, muss die Active Directory-Instanz auf einer öffentlichen IP-Adresse verfügbar sein. Aus Sicherheitsgründen sollte diese IP-Adresse nur

über die VSA-IP-Adresse des MSP erreichbar sein. Mobile Geräte übertragen ihre Authentifizierungsanforderungen über die VSA, um eine Active Directory-Instanz zu erreichen. Kundenunternehmen sollten *die IP-Adresse der VSA* für Server, die Active Directory-Instanzen von Kunden hosten, auf die Positivliste setzen.

- SSL/TLS aktiviert

Anforderungen für WebDAV-Server

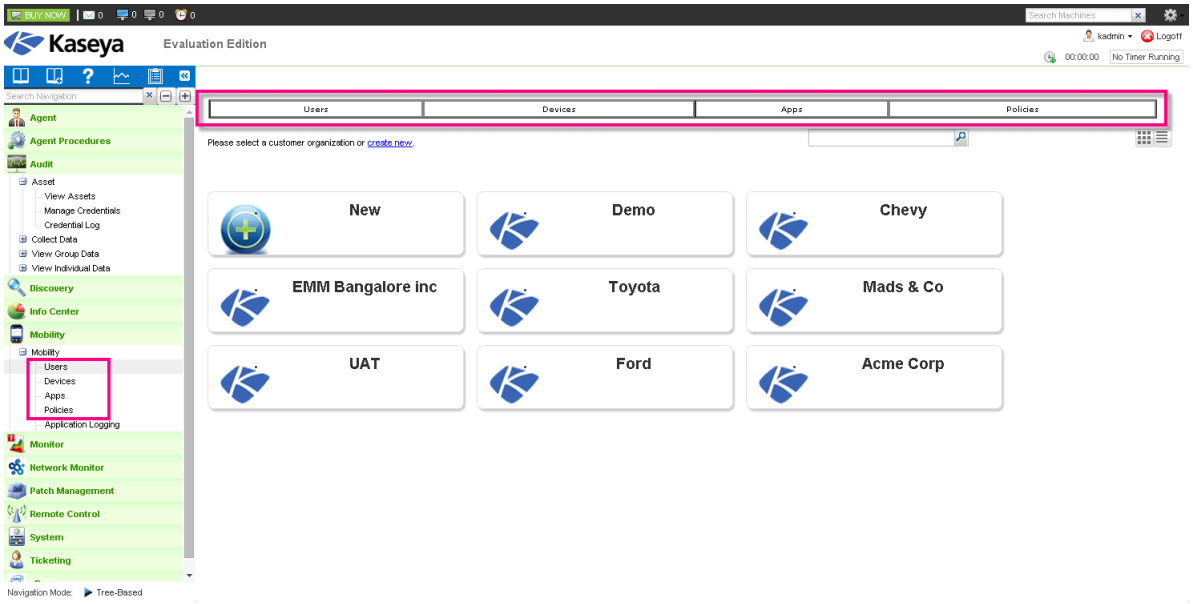
- NTLM aktiviert, wenn Authentifizierung erforderlich ist.
- VSA-Host muss Zugriff auf WebDAV-Server haben. Wenn VSA nicht dasselbe Intranet wie ein WebDAV-Server nutzt, muss der WebDAV-Server auf einer öffentlichen IP-Adresse verfügbar sein. Aus Sicherheitsgründen sollte diese IP-Adresse nur über die VSA-IP-Adresse erreichbar sein. Mobile Geräte übertragen ihre Authentifizierungsanforderungen über die VSA, um WebDAV-Server zu erreichen. Kundenunternehmen sollten die *IP-Adresse der VSA* für Server, die WebDAV-Server hosten, auf die Positivliste setzen.

Benutzeroberfläche

Enterprise Mobility Management wird als **Mobility**-Modul im Navigationsfeld der VSA identifiziert. Das Modul ist um eine einzelne integrierte Benutzeroberfläche angeordnet. Dieselben vier Hauptfunktionen verlaufen entlang des oberen Bereichs jeder Seite oder entlang der Seite des Navigationsfeldes:

- Benutzer
- Geräte
- Anwendungen
- Richtlinien

Wenn Sie das **Mobility**-Modul zum ersten Mal aufrufen, wird eine Kachelansicht der vorhandenen Kundenunternehmen, ähnlich wie in der Abbildung unten dargestellt, anzeigt. *Jeder im* **Mobility***-Modul durchgeführte Task beginnt mit dieser Benutzeroberfläche.*



Konfigurieren der Active Directory Integration

Enterprise Mobility Managementverwendet die Active Directory-Instanz eines Kundenunternehmens, um die Benutzer zu identifizieren, die zur Registrierung ihrer mobilen Geräte eingeladen wurden. Sicherheitsrichtlinien in**Enterprise Mobility Management**werden auf ein Gerät basierend auf dessen Zuordnung zu einem Active Directory-Benutzer angewendet.

Schlüsselkonzepte zur Integration

- Kundenunternehmen müssen über Active Directory verfügen, um Benutzer zu Enterprise Mobility Management hinzuzufügen. Zusätzliche Active Directory-Anforderungen finden Sie unter **Enterprise Mobility Management Modulvoraussetzungen** *(siehe 2)*.
- Benutzerdatensätze werden aus Active Directory in **Enterprise Mobility Management** importiert.
- Die Sicherheitsgruppe, der ein Benutzer in Active Directory angehört, bestimmt das Richtlinienprofil, das ihm in **Enterprise Mobility Management** zugeordnet wird. Durch das Verschieben eines Benutzers in eine andere Sicherheitsgruppe in Active Directory wird dieser Benutzer einem anderen Richtlinienprofil in **Enterprise Mobility Management** zugeordnet.
- Geräte werden den Benutzern zugeordnet, wenn diese den Kaseya Agent unter Verwendung des eindeutigen Aktivierungscodes, den sie per E-Mail erhalten haben, auf Ihren Geräten installieren und sich registrieren.
- Die mobilen Geräte des Benutzers benötigen für die Authentifizierung keinen Zugriff auf Active Directory. Eine Anwendungsanfrage wird von dem Gerät an **Enterprise Mobility Management** gesendet, welches die Anfrage an Active Directory übermittelt.
- Die AD-Authentifizierungskomponente in **Enterprise Mobility Management**speichert keine Benutzer-Anmeldedaten, sondern wirkt nur als Relais für die AD-Authentifizierung.

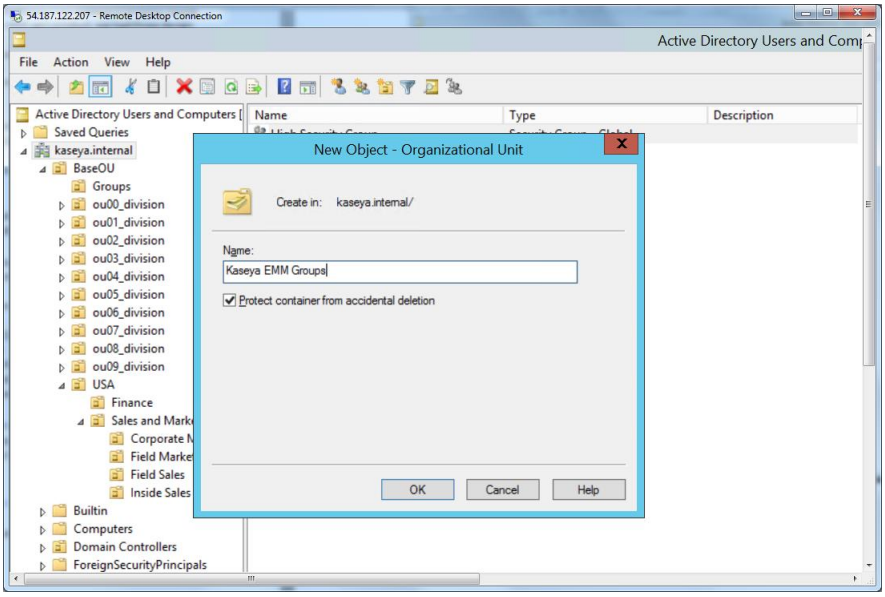
Erstellen von drei Sicherheitsgruppen in Active Directory

Enterprise Mobility Management erfordert die Erstellung von drei Sicherheitsgruppen in Active Directory. Diese werden den drei Sicherheitsgruppen in **Enterprise Mobility Management** zugeordnet:

- `Sicherheitsrichtlinie "Hoch"`
- `Sicherheitsrichtlinie "Mittel"`
- `Sicherheitsrichtlinie "Niedrig"`

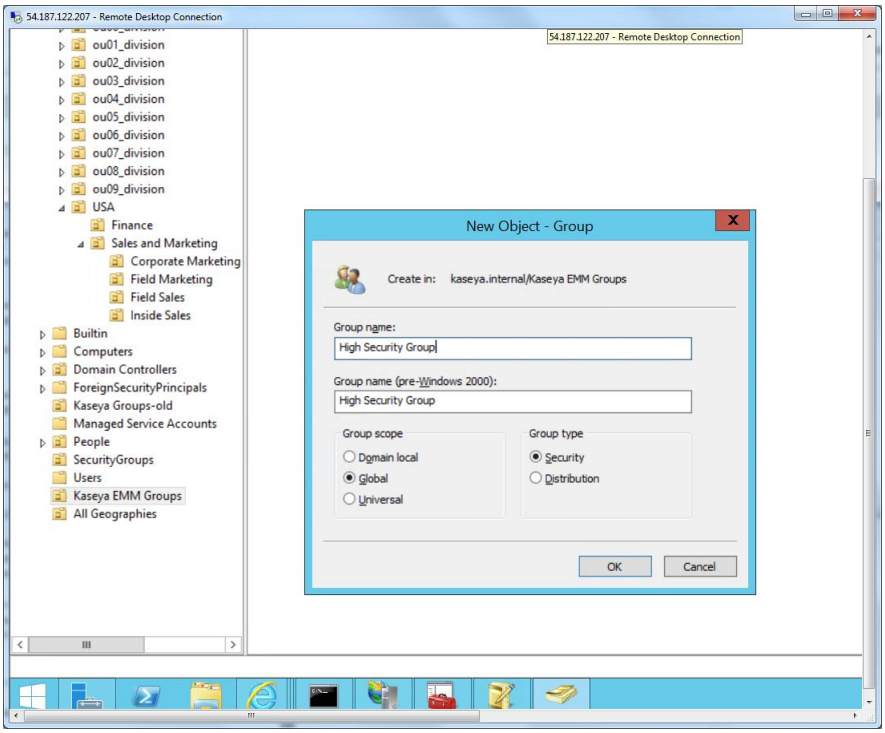
Alle Benutzerdatensätze, die für den Import in **Enterprise Mobility Management** vorgesehen sind, müssen in einer dieser drei Sicherheitsgruppen enthalten sein.

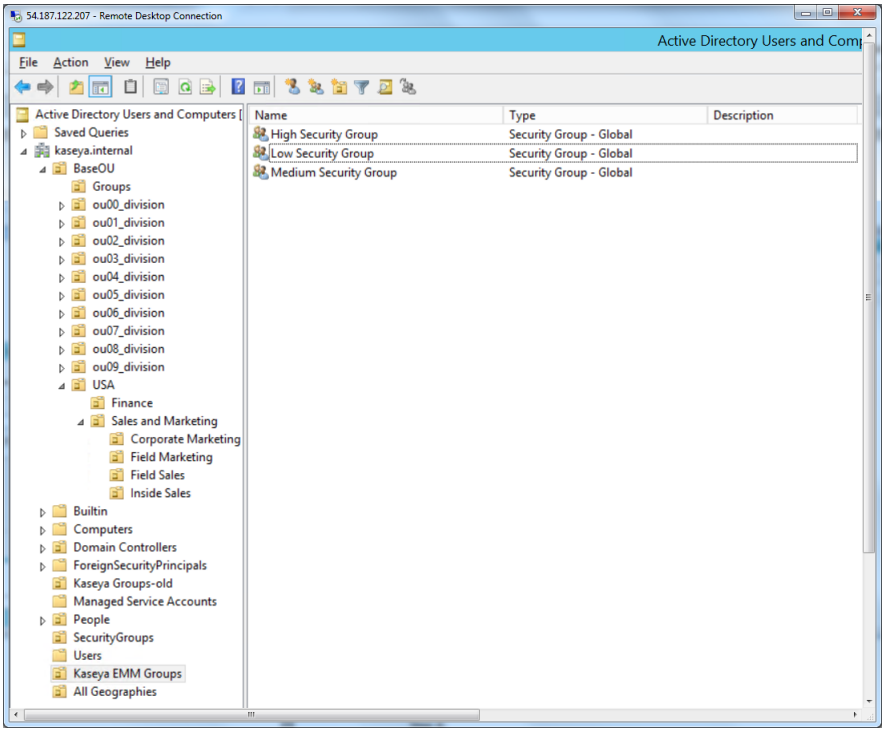
1. Öffnen Sie die Active Directory-Konsole und erstellen Sie eine neue *Organisation* mit dem Namen `Kaseya EMM Groups` unter der Hauptdomäne.



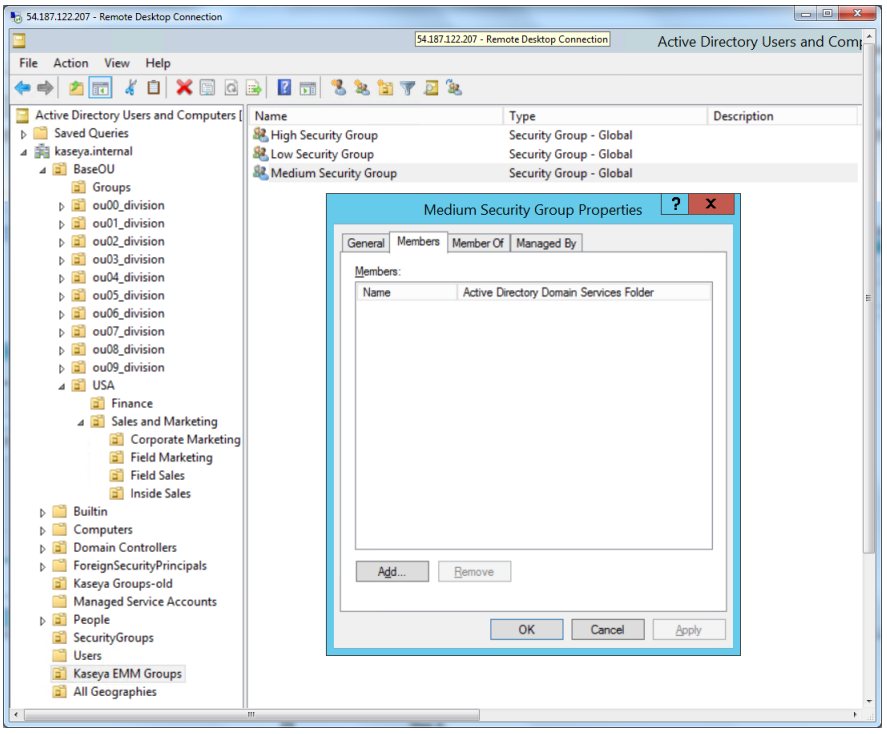
2. Erstellen Sie unter `Kaseya EMM Groups` drei Sicherheitsgruppen. Nennen Sie sie `High Security Group`, `Medium Security Group` und `Low Security Group`.

Hinweis: Sie können diese Sicherheitsgruppen anders benennen. Um das Mapping mit **Enterprise Mobility Management** zu erleichtern, empfehlen wir jedoch die Verwendung dieser Namen.

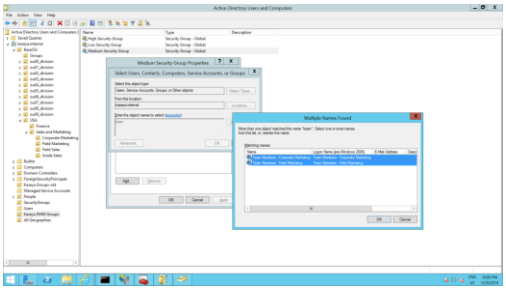




3. Klicken Sie mit der rechten Maustaste auf die drei `Kaseya EMM Groups`, klicken Sie dann auf die Option `Properties`. Öffnen Sie die Registerkarte `Members`, klicken Sie dann auf die Schaltfläche `Add`.



4. Suchen Sie in Active Directory nach Benutzern, um sie zu jeder der drei `Kaseya EMM Groups` hinzuzufügen.



Nun haben Sie die drei EMM-Sicherheitsgruppen (Hoch, Mittel und Niedrig) erstellt und ihnen die entsprechenden Benutzer zugeordnet.

5. Nachdem die Konfiguration abgeschlossen ist, sollten Sie Folgendes notieren. Diese Informationen sind erforderlich, um eine Verbindung mit einer beliebigen Instanz von Active Directory herzustellen, die Sie einem Unternehmen in **Enterprise Mobility Management** zuordnen möchten.
   - Der Domain-Name oder die IP-Adresse des Active Directory-Servers.
   - Der von Active Directory verwendete LDAP-Port. Der Standard-LDAP-Port ist 389. Der Standard-SSL-LDAP-Port ist 636.
   - Der Basis-DN (eindeutiger Name), nach dem Sie suchen müssen: Beispiel: `OU=Kaseya EMM Groups,DC=company,DC=com`
   - Die Anmeldedaten, die Sie verwenden müssen, um den Lesezugriff zu diesem eindeutigen Namen zu authentifizieren. Es werden dedizierte Anmeldedaten empfohlen.

Onboarding-Kunden

Kundenunternehmen müssen zu **Enterprise Mobility Management** hinzugefügt werden, bevor Benutzer dazu eingeladen werden, Ihre Geräte zu registrieren.

Voraussetzung: Bevor Sie beginnen, muss für jedes Kundenunternehmen, das Sie hinzufügen, *eine Active Directory-Instanz konfiguriert sein, um die Integration mit* **Enterprise Mobility Management** zu ermöglichen. Siehe **Konfigurieren der Active Directory Integration** *(siehe 4)*.

Erstellen eines neuen Unternehmens in VSA

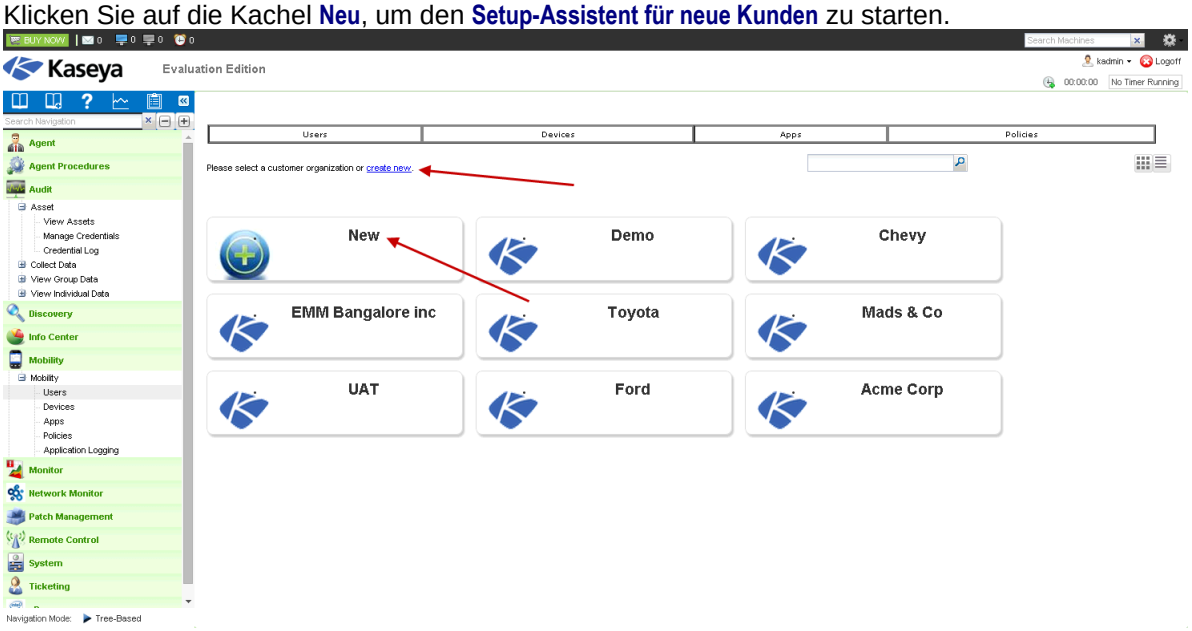
Befolgen Sie dieses Verfahren, wenn das Kundenunternehmen, das Sie hinzufügen möchten, in der gesamten VSA neu ist.

1. Navigieren Sie zur Seite System > Orgn./Gruppen/Abtlg./Personal > **Verwalten**.
2. Klicken Sie auf **Neu**, um den Dialog **Eine Organisation hinzufügen** anzuzeigen.
3. Geben Sie eine **ID** und einen **Org.-Namen** ein, um das neue Kundenunternehmen zu identifizieren.
4. Klicken Sie auf **Speichern**.

Ihr neues Kundenunternehmen wurde erstellt. Kehren Sie nun zum **Mobility**-Modul zurück, um das Kundenunternehmen zu **Enterprise Mobility Management** hinzuzufügen.

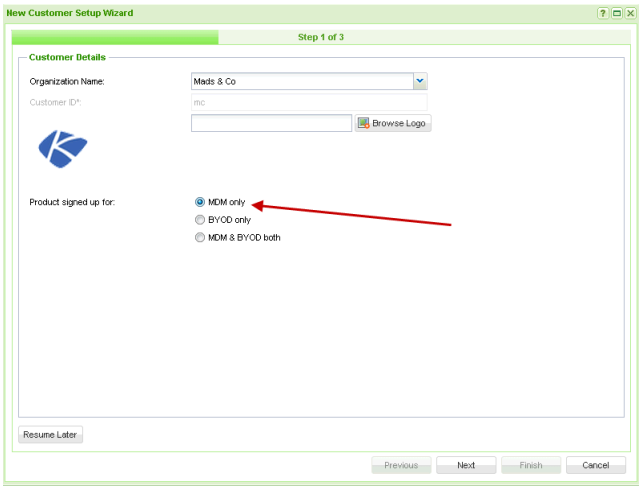
Hinzufügen eines Kundenunternehmens im Mobility-Modul

1. Klicken Sie auf die Kachel **Neu**, um den **Setup-Assistent für neue Kunden** zu starten.



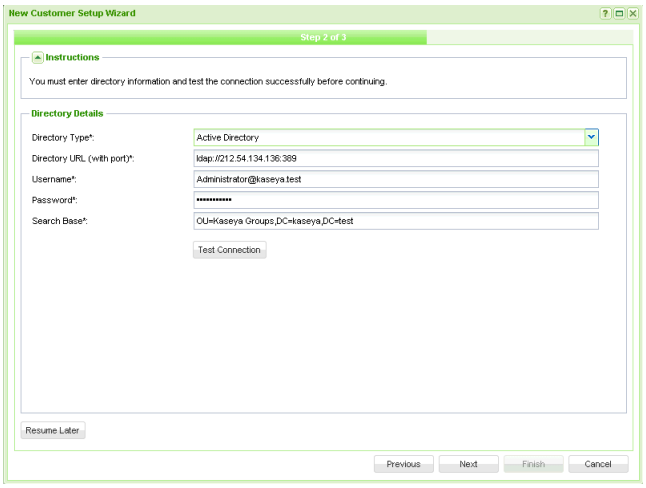
2. Wählen Sie das Kundenunternehmen aus, das Sie zum **Mobility**-Modul hinzufügen möchten.
3. Geben Sie optional ein Kundenlogo an.
4. Wählen Sie **nur MDM**, **nur BYOD** oder **MDM & BYOD beides**. Ihre Auswahl bestimmt die Richtlinienprofile und Optionen, die Ihnen auf der Benutzeroberfläche angezeigt werden, wenn dieses Kundenunternehmen ausgewählt ist.

5. Klicken Sie auf **Weiter**.



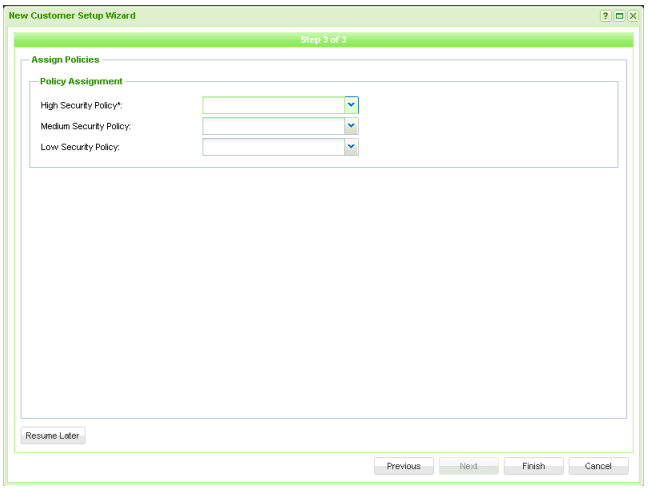
6. Geben Sie die Active Directory-Parameter an, die **Enterprise Mobility Management** verwenden soll, um Benutzer in dem Kundenunternehmen zu identifizieren.

> **Hinweis:** Für jedes Kundenunternehmen, das Sie hinzufügen, *muss eine Active Directory-Instanz konfiguriert sein, um die Integration mit* **Enterprise Mobility Management** zu ermöglichen. Siehe **Konfigurieren der Active Directory zur Integration** *(siehe 4)*.
>
> **Hinweis:** Wenn Sie Active Directory noch nicht konfiguriert haben, klicken Sie auf **Später fortsetzen**. Sie können die Kachel für dieses Kundenunternehmen anklicken, um zu diesem Schritt im Assistenten zurückzukehren. Eine Kachel des Kundenunternehmens zeigt ein Sternchen an, um anzuzeigen, dass das Active Directory-Setup noch nicht konfiguriert wurde.



- **Verzeichnistyp** – **Active Directory** ist die einzige Option.
- **Verzeichnis-URL (mit Port)** – Geben Sie eine LDAP-URL ein. Der Standardport für LDAP ist `389`. Beispiel: `ldap://212.54.134.136:389`
- **Benutzername** – Geben Sie einen Active Directory-Benutzernamen ein, der Zugriff auf den *eindeutigen Namen* ermöglicht, der im Feld **Suchbasis** angegeben ist.
- **Kennwort** – Geben Sie das Kennwort ein.
- **Suchbasis** – Geben Sie den *eindeutigen Namen* ein, der für die Suche der drei Benutzergruppen in dieser Instanz von Active Directory verwendet wird, die berechtigt sind, ihre Geräte mit **Enterprise Mobility Management** zu registrieren. Beispiel: `OU=Kaseya EMM Groups,DC=company,DC=com`

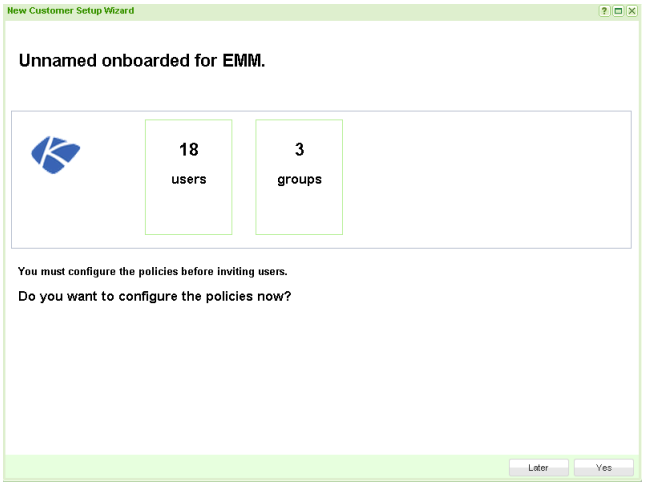
7. Klicken Sie auf die Schaltfläche **Testverbindung**, um Ihre Verbindung mit Active Directory zu überprüfen.
   - Wenn diese erfolgreich hergestellt ist, klicken Sie auf **Weiter**, um **Enterprise Mobility Management** mit den drei Benutzergruppen, die berechtigt sind, ihre Geräte mit **Enterprise Mobility Management** zu registrieren, aufzufüllen.
   - Wenn der Test fehlschlägt, überprüfen Sie, ob die auf der Assistenten-Seite eingegebenen Werte mit Ihrer Konfiguration von Active Directory übereinstimmen. Der Test muss erfolgreich sein, um mit dem Onboarding dieses Kundenunternehmens fortzufahren.
8. Weisen Sie dem neuen Kundenunternehmen **Enterprise Mobility Management**-Richtlinien für mobile Geräte zu.
   - Sie können jedem Kundenunternehmen, das Sie in **Enterprise Mobility Management** registrieren, jeweils eine Richtlinie für `Hoch`, `Mittel` und `Niedrig` zuweisen.
   - Wählen Sie die Standardrichtlinien für `Hoch`, `Mittel` und `Niedrig`, wenn Sie noch keine kundenspezifischen Richtlinien erstellt haben.



9. Die letzte Seite des Assistenten gibt Zählungen für die Benutzer und Gruppen an, die von der Active Directory-Suche zurückgegeben werden. Diese Benutzer und Gruppen wurden in **Enterprise Mobility Management** importiert. Sie erhalten Aufforderungen mit zwei Auswahlmöglichkeiten:
   - Klicken Sie auf **Später**, um die vordefinierten Standardrichtlinien für diese neu integrierten Kundenunternehmen zu übernehmen. *Diese Option umgeht die Einstellung von benutzerdefinierten Eigenschaften, die spezifisch für dieses Kundenunternehmen sind.*

     Hinweis: Möglicherweise möchten Sie Benutzer sofort dazu einladen, ein mobiles Gerät mit **Enterprise Mobility Management** zu registrieren. Weitere Einzelheiten finden Sie unter **Onboarding von Benutzern** *(siehe 11)*.
   - Klicken Sie auf **Ja**, um *neue kundenspezifische Richtlinien zu konfigurieren, die sowohl vordefinierte als auch anpassbare Eigenschaften beinhalten.*

Hinweis: Weitere Einzelheiten zur Auswahl dieser Option finden Sie unter **Konfigurieren von Richtlinien** *(siehe 18)*.



Onboarding von Benutzern

Benutzer werden automatisch dazu eingeladen, einen Kaseya-Agent auf ihren mobilen Geräten zu installieren, sobald die Benutzer aus Active Directory in Enterprise Mobility Management (siehe 8) importiert wurden. Der Benutzerstatus zeigt bereits `Eingeladen` an, wenn Sie die aufgeführten Benutzer auf dieser Seite zum ersten Mal sehen. Möglicherweise möchten Sie einen Benutzer erneut einladen, wenn er die ursprüngliche E-Mail-Einladung nicht erhalten hat.

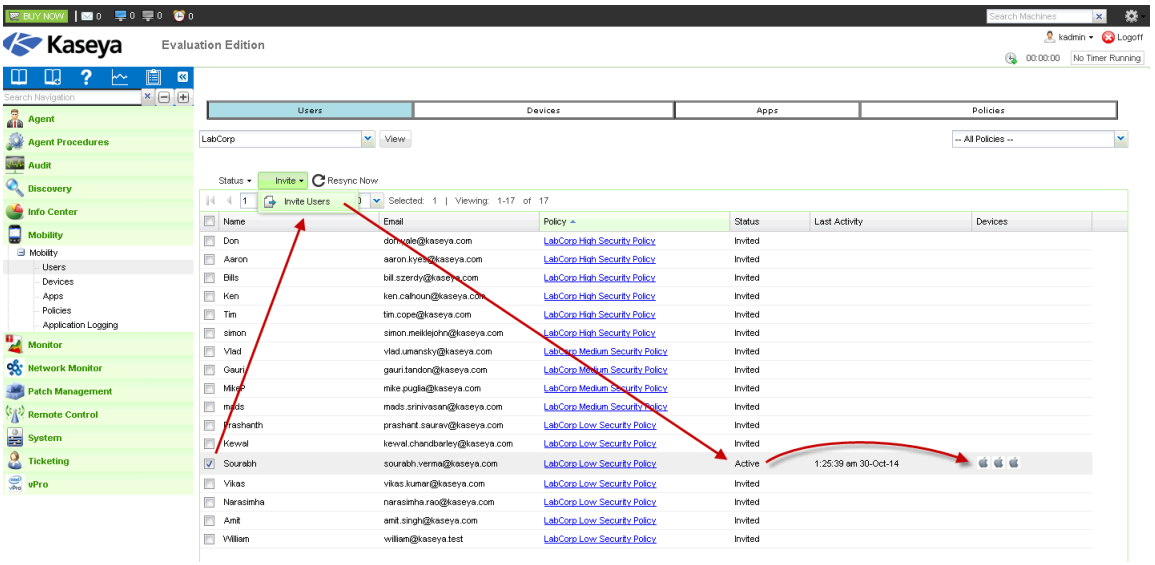
So laden Sie Benutzer erneut ein:

1. Navigieren Sie zur Seite **Benutzer**.
2. Wählen Sie einen oder mehrere Benutzer aus.

   Hinweis: Wenn ein von Ihnen erwarteter Benutzer nicht angezeigt wird, können Sie auf die Schaltfläche **Jetzt erneut synchronisieren** klicken. Dadurch wird eine erneute Verbindung mit der Active Directory-Instanz des Kundenunternehmens hergestellt und die Liste von Benutzern für das ausgewählte Kundenunternehmen aktualisiert.

3. Klicken Sie auf die Einladeoption > **Benutzer einladen**.
   - Die Spalte **Status** zeigt `Eingeladen` an, wenn eine Einladung an den Benutzer gesendet wurde.
   - Die Spalte **Status** zeigt `Aktiv` an, wenn der Benutzer den **Enterprise Mobility Management**-Agent auf einem oder mehreren Geräten installiert hat.
   - Die Anzahl der Geräte, die von **Enterprise Mobility Management** für den betreffenden Benutzer verwaltet werden, wird durch die Gerätesymbole in der Spalte **Geräte** angezeigt.

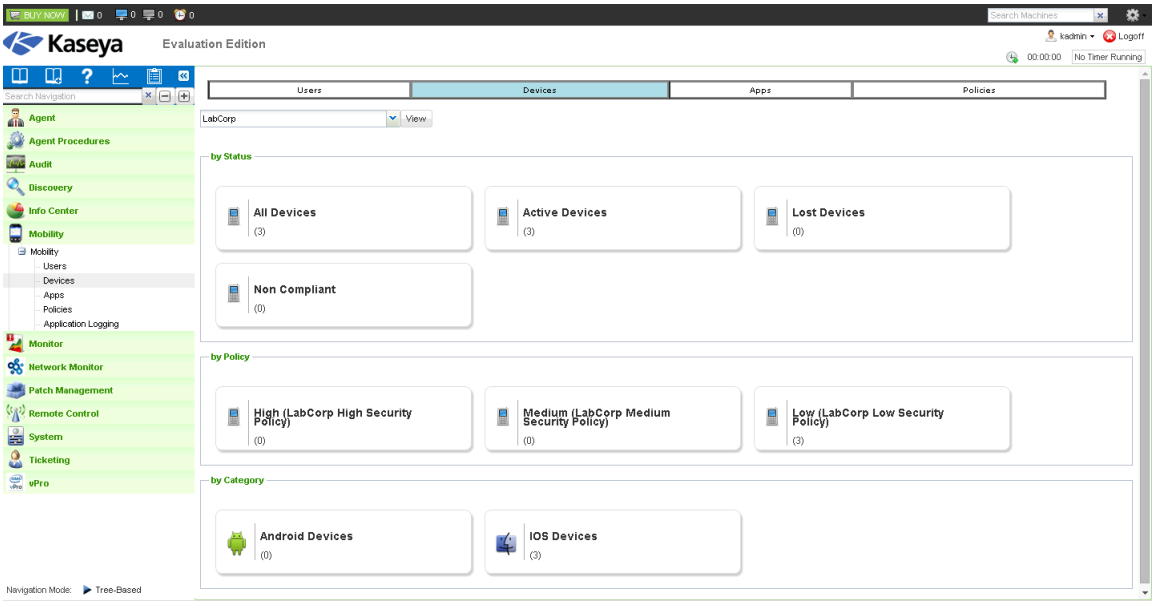
> **Hinweis:** Nähere Informationen zur Verwaltung von mobilen Geräten finden Sie unter **Verwalten von Geräten** *(siehe 12)*.



Verwalten von Geräten

Sobald Benutzer Geräte mit **Enterprise Mobility Management** registriert haben, können Sie deren Geräte verwalten.

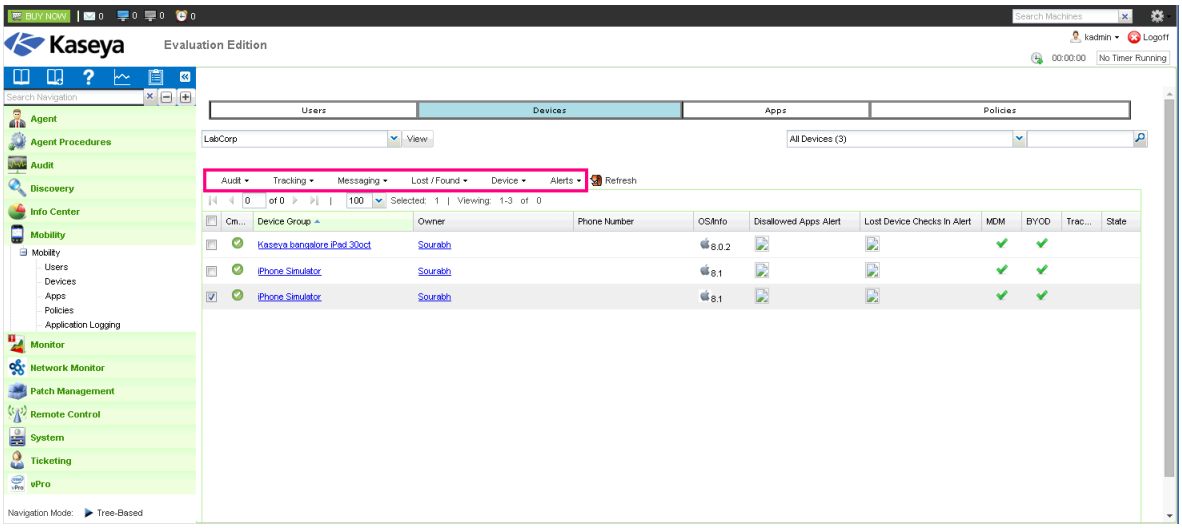
1. Navigieren Sie zu der Seite **Geräte**.
2. Wählen Sie ein Kundenunternehmen.
3. Wählen Sie eine der folgenden Kacheln aus. Kacheln sind nach folgenden Kriterien geordnet:
   - **nach Status**
   - **nach Richtlinie**
   - **nach Kategorie**



Eine Liste der Geräte für die ausgewählte Filterung wird angezeigt.

4. Wählen Sie eine oder mehrere Reihen in der Liste der Geräte aus, um alle Registerkarten oben in der Tabelle zu aktivieren.

> **Hinweis:** Durch Klicken auf den Link unter einem Gerätenamen auf der Seite **Geräte** werden die Details dieses Geräts in einer Reihe von Registerkarten angezeigt. Weitere Informationen finden Sie unter **Gerätedetails** *(siehe 15)*.



5. Durch Klicken auf das **Befehls**symbol für ein Gerät in der Geräteliste wird das Fenster **Befehlsstatus** *(siehe 13)* angezeigt.
6. Die Aktionen, die Sie ausführen können, sind in den folgenden Registerkarten geordnet. Nähere Informationen erhalten Sie in den folgenden Themen.
   - **Audit** *(siehe 14)*
   - **Nachverfolgung** *(siehe 14)*
   - **Nachrichten** *(siehe 14)*
   - **Verloren/Gefunden** *(siehe 14)*
   - **Geräte** *(siehe 15)*
   - **Meldungen** *(siehe 15)*

Befehlsstatus

Durch Klicken auf das **Befehls**symbol für ein Gerät in der Geräteliste wird das Fenster **Befehlsstatus** angezeigt. Dieses Fenster zeigt den Status der Befehle an, die an ein Gerät gesendet wurden.

- - Der Befehl ist ausstehend. Der Agent hat sich noch nicht zum Abrufen angemeldet.
- - Der Agent bearbeitet den Befehl.
- - Der Vorgang ist abgeschlossen.
- - Befehl fehlgeschlagen.

Verwenden Sie die Option **Als abgeschlossen kennzeichnen**, um einen oder mehrere Befehle auf abgeschlossen zu setzen .

Audit-Aktionen

Audits werden durchgeführt, sobald der Benutzer einen Kaseya-Agent auf seinem mobilen Gerät installiert. Danach werden Audits standardmäßig täglich durchgeführt.

- **Ein Audit planen** – Plant ein Audit für eine bestimmte Zeit auf ausgewählten Geräten. Planen Sie eine einmalige oder periodische Ausführung. Jede Art der Wiederholung (täglich, wöchentlich, monatlich) zeigt weitere Optionen für diese Art der Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen.
- **Audit jetzt ausführen** – Führt sofort ein Audit eines ausgewählten Geräts aus.
- **Protokolle anfordern** – *Das Geräteprotokoll dient nur für Kaseya Support-Zwecke.* Das Geräteprotokoll zeigt die tatsächlichen Nachrichten an, die zwischen VSA und einem ausgewählten Gerät hin- und her gesendet wurden.

Nachverfolgungsaktionen

Sie können auf einem Gerät alle folgenden **Nachverfolgungs**-Aktionen durchführen.

- **Nachverfolgung aktivieren** – Startet das Standort-Tracking der ausgewählten Geräte. Nach dem Start können Sie das Gerät auf einer Karte mithilfe der Registerkarte **Standort** eines Geräts nachverfolgen. Siehe **Gerätedetails anzeigen** *(siehe 15)*
- **Nachverfolgung deaktivieren** – Stoppt das Standort-Tracking der ausgewählten Geräte.
- **Aktuellen Standort abfragen** – Gibt den aktuellen Standort eines ausgewählten Geräts auf Anfrage aus, aber verfolgt ihn nicht kontinuierlich nach.
- **Standortverlauf** – Zeigt den Standortverlauf eines Geräts an.

Messaging-Aktionen

Sie können auf einem Gerät alle folgenden **Messaging**-Aktionen durchführen.

- **Ansicht** – Zeigt den Verlauf der an den Benutzer gesendeten Meldungen an.
- **Senden** – Zeigt ein Dialogfenster zur Eingabe und Sendung einer Textnachricht an den Benutzer an.

Verloren/Gefunden-Aktionen

Sie können auf einem Gerät alle folgenden **Verloren/Gefunden**-Aktionen durchführen.

- **Gestohlenalarm auf Gerät auslösen** – Nach dem Anklicken zeigen ausgewählte Geräte bei jedem Einschalten "Dieses Telefon ist gestohlen". Siehe **Alarm stummschalten** unten.
- **Daten löschen** – Bei Anklicken werden ausgewählte Geräte zurück auf ihre Standardeinstellungen gesetzt. **Beim Löschen eines Geräts werden alle Benutzerdaten** gelöscht, einschließlich der *MobileManage*-Anwendung. Die *MobileManage*-Anwendung kann sich nach dem Löschen des Geräts nicht mehr anmelden.
- **Passcode löschen** – Setzt Passcodes auf *Geräteebene* auf verwalteten iOS-Geräten zurück. Durch ein Zurücksetzen wird das Gerät entsperrt, wodurch der Benutzer das Gerät entweder ohne Passcode verwenden oder einen neuen Passcode einstellen kann. Durch Löschen des Passcodes wird das darunterliegende Sicherheitsprofil nicht geändert. Wenn das Gerät so konfiguriert ist, dass ein Passcode auf Geräteebene erforderlich ist, so wird der Benutzer direkt dazu aufgefordert, einen neuen einzugeben.

- **Check-in anfordern** – Benutzer der ausgewählten Geräte werden angewiesen, auf das Symbol der *MobileManage*-Anwendung zu tippen, um sie zu öffnen. Durch Öffnen der *MobileManage*-Anwendung meldet sich die Anwendung sofort an.
- **Als verloren markieren** – Kennzeichnet das Gerät als verloren.
- **Als gefunden markieren** – Kennzeichnet das Gerät als gefunden.
- **Alarm stummschalten** – Hält Alarme an, die mit der Aktion **Gestohlenalarm auf Gerät auslösen** auf ausgewählten Geräten eingestellt wurden.

Geräteaktionen

Sie können auf einem Gerät alle folgenden **Geräte**-Aktionen durchführen.

- **Gerät sperren** – Bei Anklicken werden ausgewählte Geräte gesperrt und der Benutzerzugriff verhindert.
- **Löschen** – Löscht ausgewählte Gerätekonten in <EEM2>.

Benachrichtigungsaktionen

Sie können auf einem Gerät alle folgenden **Benachrichtigungs**-Aktionen durchführen.

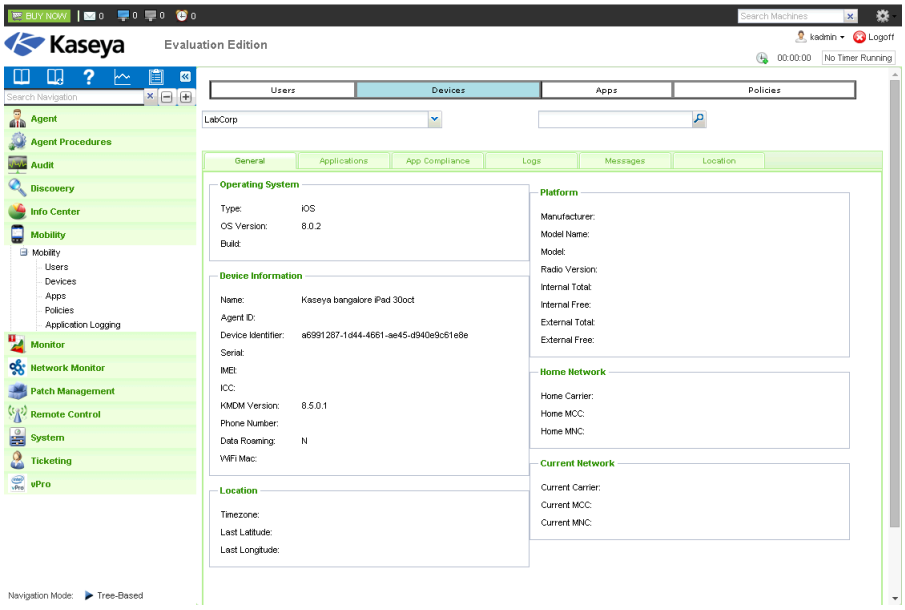
- **Details** – Zeigt ein Fenster mit **Benachrichtigungsdetails** für ausgewählte Geräte an:
  - **Benachrichtigungsname** – Der Benachrichtigungstyp: `Benachrichtigung über angemeldetes verlorenes Gerät` oder `App Konformitätskontrolle`.
  - **Aktiviert** – Benachrichtigungen sind immer aktiviert.
  - **Status** – `Benachrichtigung` oder `ok`
  - **Details** – Zeigt bei einer `App-Konformitätsbenachrichtigung` die Anzahl der `erforderlichen Apps` oder `nicht zugelassenen Apps` an.
  - **Aktion** – Löst die Benachrichtigung und setzt sie in den Status OK zurück.
- **Gelöst** – Löst Benachrichtigungen nach Benachrichtigungstyp für ausgewählte Geräte. Durch Lösen einer Benachrichtigung werden die Benutzer ausgewählter mobiler Geräte benachrichtigt.

Gerätedetails anzeigen

Durch Klicken auf den Link unter einem Gerätenamen auf der Seite **Geräte** werden die Details dieses Geräts in einer Reihe von Registerkarten angezeigt.

- **Allgemein**
- **Anwendung**
- **App-Konformität**
- **Protokolle**
- **Meldungen**

- **Ort**



Registerkarte "Allgemein"

Betriebssystem

- **Typ** – Der Typ des Betriebssystems auf dem Gerät.
- **Betriebssystemversion** – Die Version des Betriebssystems, die das Gerät nutzt.
- **Build** – Die Build-Nummer des Betriebssystems.

Gerätedaten

- **Name** – Der Name, den das Gerät zur eigenen Identifikation verwendet.
- **Agent-ID** – Die Kaseya Agent-GUID.
- **Gerätebezeichner** – Ein eindeutiger Bezeichner, der dem Gerät vom Hersteller zugewiesen wurde.
- **Seriell** – Die Seriennummer des Geräts.
- **IMEI** – Der eindeutige Bezeichner der Haupt-Assembly des Geräts, unabhängig von der im Gerät eingelegten SIM-Karte. Die IMEI-Nummer gilt für GSM-, WCDMA- und iDEN-Mobiltelefone.
- **ICC** – Der eindeutige Bezeichner der in ein Gerät eingelegten SIM-Karte.
- **KMDM-Version** – Die Version der *MobileManage*-Anwendung auf dem Gerät.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Datenroaming** - `Wahr` oder `Falsch`.
- **WiFi MAC** – Die MAC ID des Geräts.

Ort

- **Zeitzone** – Die Zeitzone, die das Gerät verwendet.
- **Letzte geografische Breite** – Die letzte geografische Breite, die das Gerät ausgegeben hat.
- **Letzte geografische Länge** – Die letzte geografische Länge, die das Gerät ausgegeben hat.

Plattform

- **Hersteller** – Der Hersteller der Gerätehardware.

- **Modellname** – Der Modellname der Gerätehardware.
- **Modell** – Die Modellnummer der Gerätehardware.
- **Funkversion** – Die Version der Modem-Firmware, die das Gerät nutzt. Wird auch als "Basisband" bezeichnet.
- **Intern gesamt** – Der gesamte verfügbare Speicherplatz auf der Hardware.
- **Intern frei** – Auf der Hardware verfügbarer und freier Speicherplatz.
- **Extern gesamt** – Der gesamte verfügbare externe Speicherplatz .
- **Extern frei** – Extern verfügbarer und freier Speicherplatz.

Heimat-Netzwerk

- **Original-Netzbetreiber** – Der Hauptdienstanbieter des Geräts.
- **Home-MCC** – Der originale Mobile Country Code des Geräts. Große Länder können mehr als einen Mobile Country Code haben.
- **Home-MNC** – Der Mobile Network Code für den Originalbetreiber/Carrier des Geräts.

Aktuelles Netzwerk

- **Aktueller Netzbetreiber** – Der Netzbetreiber, den das Gerät derzeit verwendet.
- **Aktueller MCC** – Der Mobile Country Code, den das Gerät derzeit verwendet.
- **Aktueller MNC** – Der Mobile Network Code des Betreibers/Carrier, den das Gerät derzeit verwendet.

Registerkarte "Anwendungen"

Die Registerkarte **Anwendungen** zeigt eine Liste der Anwendungen an, die auf dem ausgewählten verwalteten mobilen Gerät installiert sind.

Registerkarte "App-Konformität"

In der Registerkarte **App-Konformität** werden **Erforderliche Apps, die auf Gerät fehlen** angezeigt.

- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.

Registerkarte "Protokolle"

Die Registerkarte **Protokolle** zeigt Einträge von Geräteprotokollen an. *Das Geräteprotokoll dient nur für Kaseya Support-Zwecke.* Das Geräteprotokoll zeigt die tatsächlichen Nachrichten an, die zwischen VSA und einem ausgewählten Gerät hin- und her gesendet wurden.

Meldungen

Die Registerkarte **Meldungen** zeigt einen Verlauf der Meldungen an, die vom und zum Gerät gesendet wurden.

- **Richtung**
  - - vom Gerät gesendet
  - - vom VSA-Administrator gesendet
- **Datum** – Datum/Uhrzeit der Meldung.
- **Von** – *Gilt nur für Gerätemeldungen.* Der Gerätebezeichner und die Rechnergruppe.
- **Meldung** – Der Text der Nachricht.

Ort

Die Registerkarte **Standort** zeigt Standortverfolgungsdaten für ein ausgewähltes Gerät an. Jede nummerierte Markierung auf der Karte bezieht sich auf eine nummerierte Liste auf der rechten Kartenseite. Die nummerierte Liste gibt Datum und Zeit an, wann sich das Gerät an dem Ort befunden

hat. Die Datenanzeige wird durch einen bestimmten Datums- und Uhrzeitbereich gefiltert.

Hinweis: Wenn Sie keine Standortmarkierung eines Geräts sehen, das Sie nachverfolgen, versuchen Sie, den Filter zurückzusetzen, sodass ein früherer Datumsbereich angezeigt wird.

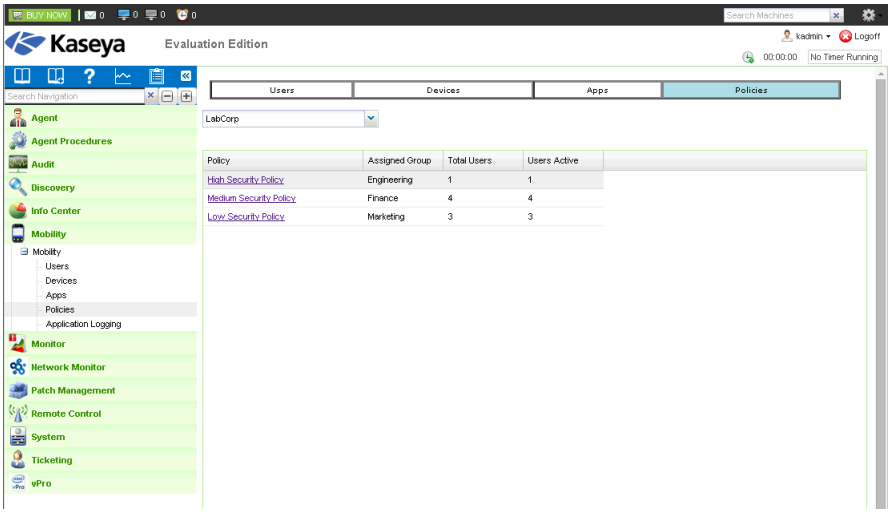
- **Datum und Zeit** – Ändern Sie bei Bedarf den Datums- und Zeitfilter. Der Filter begrenzt die Anzeige der Gerätestandorte auf einen Datums- und Uhrzeitbereich.
- **Aktualisieren** – Aktualisieren Sie die Karte nach Zurücksetzen des Filters **Datum und Zeit**.

Regeln konfigurieren

Die Seite **Richtlinien** weist **Enterprise Mobility Management**-Richtlinien nach Kundenunternehmen und Active Directory-Sicherheitsgruppe zu.

Sie können jede Richtlinie anpassen, um:

- Vordefinierte Richtlinieneinstellungen zu überprüfen.
- Eine neue Richtlinie zu erstellen und anpassbare Einstellungen für dieses Kundenunternehmen zu konfigurieren.



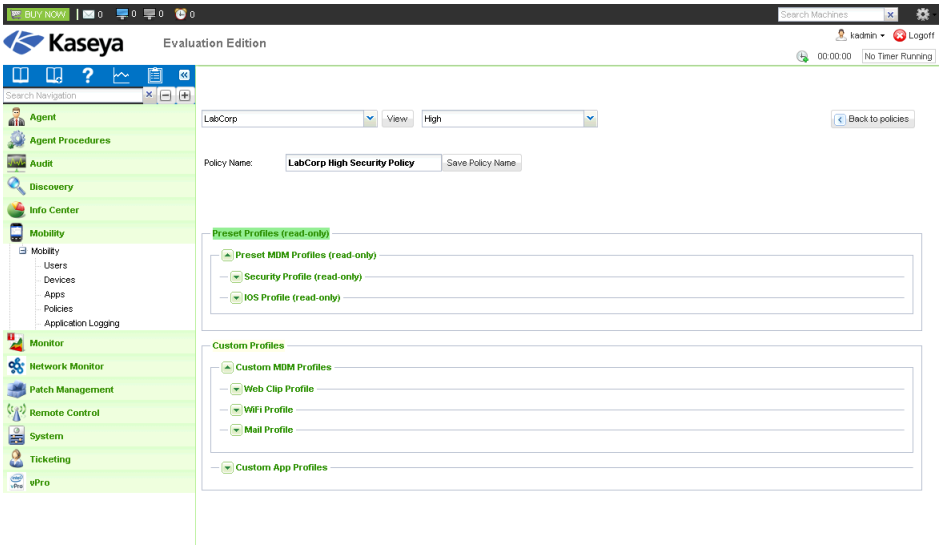
Erstellen und Konfigurieren einer neuen Richtlinie

1. Wählen Sie auf der Seite **Richtlinien** das anzuzeigende Kundenunternehmen aus.
2. Klicken Sie auf den Link zu einer der aufgeführten Richtlinien.

   Auf den Details-Seiten werden zwei Typen von Profilen angezeigt:

   - **Voreingestellte Profile (schreibgeschützt)** – Kaseya hat die korrekten Einstellungen für diese Eigenschaften festgelegt. Sie müssen nicht angepasst werden. Jede Art der Richtlinie – `Hoch`, `Mittel` und `Niedrig` – hat etwas andere Profileinstellungen.

- **Benutzerdefinierte Profile** – Diese Einstellungen sind kundenspezifisch. *Erstellen Sie immer eine neue Richtlinie anstatt diese Eigenschaften auf die Standardrichtlinien* `Hoch`, `Mittel` *und* `Niedrig` *einzustellen.*



3. Geben Sie einen neuen Namen in das Feld **Name der Richtlinie** ein. Für das Unternehmen `Acme` können Sie zum Beispiel `Acme High Security Policy` eingeben.
4. Bestätigen Sie, dass die richtige *Art der Richtlinie* ausgewählt ist: `Hoch`, `Mittel` oder `Niedrig` in der Drop-down-Liste. Ändern Sie bei Bedarf auf die richtige Art der Richtlinie.
5. Klicken Sie auf die Schaltfläche **Richtliniennamen speichern**.

   Sie haben nun eine neue Richtlinie erstellt und dem ausgewählten Kundenunternehmen zugeordnet.
6. Erweitern Sie die **Benutzerdefinierten MDM-Profile**, um die Konfigurationsdetails eines der folgenden Profile hinzuzufügen:
   - **Web Clip-Profil** *(siehe 19)*
   - **WiFi-Profil** *(siehe 20)*
   - **E-Mail-Profil** *(siehe 20)*
7. Erweitern Sie die **Benutzerdefinierten App-Profile**, um eine oder mehrere Anwendungen zum benutzerdefinierten App-Profil für dieses Kundenunternehmen hinzuzufügen. Diese Funktion wird unter den folgenden Themen ausführlich beschrieben:
   - **Verwalten von Anwendungen auf Geräten** *(siehe 26)*
   - **Konfigurieren des App-Katalogs** *(siehe 26)*
   - **Konfigurieren der App-Profile in einer Richtlinie** *(siehe 23)*
8. Erweitern Sie die **Benutzerdefinierten BYOD-Profile**, um die Konfigurationsdetails zum sicheren Zugriff auf die internen Websites und Dokumente eines Kundenunternehmens hinzuzufügen.
   - **URL-Profil** *(siehe 21)*
   - **Dokumentprofil** *(siehe 21)*
   - **Proxy-Listenprofil** *(siehe 21)*

Benutzerdefinierte MDM-Richtlinien

Konfigurieren eines Web Clip-Profils

- Dieser Profiltyp wird auf iOS-Geräten unterstützt. Bei iOS-Geräten muss die URL mit HTTP oder HTTPS

beginnen
- Dieses Profil wird auf Android nicht unterstützt.

Das **Web Clip-Profil** gibt eine Webanwendungsverknüpfung zu einer URL an, auf die das Gerät zugreifen kann. Ein Unternehmen kann Verknüpfungen auf Geräten installieren, die direkt zu seinen Websites oder Supportdokumenten führen.

- **Name** – Der Name des Profils.
- **Beschreibung** – Die Beschreibung des Profils.
- **URL** – Die URL der Webanwendungsverknüpfung.
- **Bezeichnung** – Ein Anzeigename für die Webanwendungsverknüpfung.
- **Symbol** – Lädt eine png-Datei hoch, die als Symbol für die Verknüpfung dient.
- **Ist entfernbar** – Bei Markierung kann der Benutzer die Webanwendungsverknüpfung löschen.

Konfigurieren eines WiFi-Profils

- Dieser Profiltyp wird auf iOS- und Android-Geräten unterstützt:

Das **WiFi-Profil** stellt die WiFi-Optionen auf Geräten ein.

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **SSID** – Ein eindeutiger Bezeichner eines drahtlosen Netzwerks.
- **Ausgeblendetes Netzwerk** – Bei Markierung sendet das drahtlose Netzwerk seine SSID nicht.
- **Verschlüsselungstyp** – Der Verschlüsselungstyp, der vom drahtlosen Netzwerk verwendet wird. Stellen Sie sicher, dass diese Werte genau mit den Eigenschaften des Netzwerkzugriffspunkts übereinstimmen. Wenn Sie bezüglich des Verschlüsselungstyps unsicher sind oder möchten, dass er für alle Verschlüsselungstypen gilt, verwenden Sie den Wert `Any`.
  - `WEP` – Wired Equivalent Privacy
  - `WPA` – WiFi Protected Access. Schließt sowohl WPA als auch WPA2 ein.
  - `Alles` – Alle anderen Arten von WiFi-Protokollen
- **Kennwort** – Das WiFi-Kennwort.

Konfigurieren eines E-Mail-Profils

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Falls die Felder für Benutzeranzeigename, E-Mail-Adresse, Benutzername oder Kennwort leer sind, werden sie aus dem Gerätedatensatz ausgefüllt.
- Dieser Profiltyp wird teilweise auf Android-Geräten unterstützt.

Das **E-Mail-Profil** konfiguriert den E-Mail-Client auf einem verwalteten mobilen Gerät.

- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Kontotyp** – `IMAP`, `POP`, `Gmail` oder `Exchange`. Die Option `Gmail` ist eine vordefinierte IMAP-Konfiguration eines Gmail-Kontos. Nur die Felder "Benutzername" und "Kennwort" müssen ausgefüllt werden, um diese `Gmail`-IMAP-Konfiguration abzuschließen. Siehe **Konfigurieren eines Exchange E-Mail-Profils** unten.
- **Benutzeranzeigename** – Der Anzeigename des E-Mail-Kontos.

  Hinweis: Wenn bei iOS die Felder **Benutzeranzeigename** und **E-Mail-Adresse** leer gelassen werden, wird der Gerätebenutzer dazu aufgefordert, seinen Benutzernamen und seine E-Mail-Adresse einzugeben, wenn das Profil auf dem Gerät angewendet wird.

- **E-Mail-Adresse** – Die E-Mail-Adresse des Benutzers.

- **Eingehende Server-IP oder Hostname** – Der IMAP- oder POP3-Eingangsserver. Zum Beispiel `pop.IhreMail.com` oder `imap.IhrEMailServer.com`.
- **Eingehender Server-Port** – Die vom eingehenden E-Mail-Dienst verwendete Port-Nummer. Bei POP3 in der Regel `110` oder bei aktiviertem SSL `995`. Wenn IMAP aktiviert ist, in der Regel `143` oder bei aktiviertem SSL `993`.
- **Kennwort für Eingangsserver erforderlich** – Bei Markierung ist für den Eingangsserver ein Kennwort erforderlich.
  - **Kennwort für Eingangsserver** – Geben Sie das Kennwort ein.
- **SSL für eingehende E-Mail verwenden** – Bei `Ja` wird die Kommunikation mit dem Eingangsserver mithilfe von SSL verschlüsselt. Damit diese Funktion verwendet werden kann, muss Ihr Eingangsserver SSL unterstützen.
- **Nachrichten auf dem Server belassen** – Bei `Ja` bleiben die E-Mails auf dem Eingangsserver gespeichert, nachdem sie auf das Gerät übertragen wurden.
- **Ausgangsserver-IP oder Hostname** – Der SMTP-Ausgangsserver. Zum Beispiel `smtp.IhrEMailServer.com`.
- **Ausgangsserver-Port** – Die Port-Nummer, die der Ausgangsserver verwendet. In der Regel `25` oder bei aktiviertem SSL `465`.
- **Benutzername für Ausgangsserver** – Wenn "Ausgangs-Authentifizierung" markiert ist, der Benutzername für den Ausgangsserver.
- **Gleiches Kennwort wie für Eingangsserver verwenden** – Bei Markierung verwenden sowohl Eingangs- als auch Ausgangsserver das gleiche Eingangskennwort. Geben Sie ein Kennwort an, falls dieses Feld leer ist.
  - **Ausgangsserver-Kennwort** – Geben Sie ein Kennwort ein.
- **SSL für ausgehende E-Mail verwenden** – Bei `Ja` wird die Kommunikation mit dem Ausgangsserver mithilfe von SSL verschlüsselt. Damit diese Funktion verwendet werden kann, muss Ihr Ausgangsserver SSL unterstützen.

Konfigurieren eines Exchange E-Mail-Profils

Stellen Sie folgende Werte ein, um ein Exchange E-Mail-Profil in **Enterprise Mobility Management** zu konfigurieren:

- **Kontotyp** – Wählen Sie `Exchange`.
- **E-Mail-Adresse** – Geben Sie eine E-Mail-Adresse ein.
- **Eingehende Server-IP oder Hostname** – Geben Sie den Exchange-Serverhostnamen ein.
- **Benutzername für Eingangsserver** – Geben Sie einen Domain-Benutzernamen ein im Format `domain\benutzername`
- **Kennwort für Eingangsserver erforderlich** – Markieren Sie dieses Kontrollkästchen.
- **Kennwort** – Geben Sie das Kennwort für den Domain-Benutzernamen ein.
- **Eingehender Server-Port** – Standardeinstellungen auf `143`.
- **Ausgangsserver-Port** – Standardeinstellungen auf `25`.
- **SSL für eingehende E-Mail verwenden** – Als Standardeinstellung markiert.
- **Gleiches Kennwort wie für Eingangskennwort verwenden** – Markieren Sie dieses Kontrollkästchen.

Hinweis: *Nur bei iOS-Geräten* müssen Sie für jedes iOS-E-Mail-Profil getrennte Profile in **Enterprise Mobility Management** erstellen und Benutzernamen, E-Mail-Adresse und Kennwort angeben.

Benutzerdefinierte BYOD-Profile

Sie können drei benutzerdefinierte BYOD-Profile für eine ausgewählte Kundenunternehmen- und Active Directory-Sicherheitsgruppe konfigurieren. Erweitern Sie eines der **Benutzerdefinierten**

BYOD-Profile, um die Konfigurationsdetails für Folgendes hinzuzufügen:

- **URL-Profil**
- **Dokumentprofil**
- **Proxy-Listenprofil**

Setzen von VSA auf die Positivliste

Wenn VSA nicht dasselbe Intranet wie ein WebDAV-Server nutzt, muss der WebDAV-Server auf einer öffentlichen IP-Adresse verfügbar sein. Aus Sicherheitsgründen sollte diese IP-Adresse nur über die VSA-IP-Adresse erreichbar sein. Mobile Geräte übertragen ihre Authentifizierungsanforderungen über die VSA, um WebDAV-Server zu erreichen. Kundenunternehmen sollten die *IP-Adresse der VSA* für Server, die WebDAV-Server hosten, auf die Positivliste setzen.

URL-Profil

Fügen Sie die URLs, auf die *direkt zugegriffen werden kann*, zu einer Netzwerkverbindung eines Geräts hinzu. Benutzer verwenden den **WorkBrowser** *(siehe 28)*, um auf diese URLs zuzugreifen.

- **Name** – Geben Sie einen Namen für dieses Menüelement ein.
- **URL** – Geben Sie eine URL ein.
- **Proxy erforderlich** – Bei Markierung muss bei Zugriff auf eine Verknüpfung auf einer Webseite zu einer anderen `http://<Unterdomäne>.<Domäne>` diese Domäne im **Proxy-Listenprofil** aufgeführt sein. Anderenfalls wird dem Benutzer der Zugriff verweigert. Beispiel: Wenn **Proxy erforderlich** markiert ist, bedeutet eine Verknüpfung zu `sales.acme.com` von einer `support.acme.com`-Webseite, dass `support.acme.com` oder `*.acme.com` dem **Proxy-Listenprofil** hinzugefügt werden muss.

  Ist es nicht markiert, ist der Zugriff auf eine Verknüpfung auf einer Webseite zu einer anderen `http://<Unterdomäne>.<Domäne>` erlaubt, was ein Sicherheitsrisiko darstellen könnte.

Dokumentprofil

Fügen Sie mit **WorkDocs** *(siehe 28)* WebDAV-Dokumente hinzu, die mobilen Benutzer zur Verfügung gestellt werden sollen.

- **Name** – Eine Beschreibung des Dokuments.
- **URL** – Die URL der WebDAV-Dokumentenquelle.
- **Proxy erforderlich** – Bei Markierung muss bei Zugriff auf eine Verknüpfung in einem Dokument zu einer anderen `http://<Unterdomäne>.<Domäne>` diese Domäne im **Proxy-Listenprofil** aufgeführt sein. Anderenfalls wird dem Benutzer der Zugriff verweigert. Beispiel: Wenn **Proxy erforderlich** markiert ist, bedeutet eine Verknüpfung zu `sales.acme.com` in einem `support.acme.com`-Dokument, dass `support.acme.com` oder `*.acme.com` dem **Proxy-Listenprofil** hinzugefügt werden muss.

  Ist es nicht markiert, ist der Zugriff auf eine Verknüpfung in einem Dokument zu einer anderen `http://<Unterdomäne>.<Domäne>` erlaubt, was ein Sicherheitsrisiko darstellen könnte.

Die Container-Anwendung **WorkDocs** unterstützt:

- Anzeige und Bearbeitung freigegebener und lokaler Microsoft Office- und PDF-Dokumente.
- Erstellung und Speicherung lokaler sicherer Dokumente auf dem mobilen Gerät des Benutzers. Lokal gespeicherte Dokumente werden verschlüsselt und bleiben vom Rest der Benutzerumgebung auf dem mobilen Gerät isoliert.

Proxy-Listenprofil

Trifft zu, wenn bei einer `http://<Unterdomäne>.<Domäne>`, die dem oben angegebenen **URL-Profil** hinzugefügt wurde, das Kontrollkästchen **Proxy erforderlich** markiert ist. Gibt andere `http://<Unterdomäne>.<Domänen>` an, auf die der Benutzer zugreifen kann, wenn er auf eine Verknüpfung klickt, die in den Seiten eines **URL-Profils** `http://<Unterdomäne>.<Domänen>`- oder **Dokumentprofil**-Dokument eingebettet ist. Die Angabe *.* wird akzeptiert. Beispiel: `*.acme.com` umfasst `sales.acme.com`, `support.acme.com`, `it.acme.com`.

Benutzerdef. Anwendungsrichtlinien

Benutzerdefinierte App-Profile können einer Richtlinie zugewiesen werden. Ein benutzerdefiniertes App-Profil bestimmt, welche Anwendungen auf den verwalteten Geräten eines Kundenunternehmens entweder erforderlich oder verboten sind.

Vor dem Durchführen dieses Schritts sollten die folgenden Schritte abgeschlossen sein:

- **Verwalten von Anwendungen auf Geräten** *(siehe 26)*
- **Konfigurieren des App-Katalogs** *(siehe 26)*

Konfigurieren eines App-Profils in einer Richtlinie

1. Wählen Sie auf der Seite **Richtlinien** das anzuzeigende Kundenunternehmen aus.
2. Klicken Sie auf den Link zu einer der aufgeführten Richtlinien.
3. Erweitern Sie die **Benutzerdefinierten App-Profile**, um eine oder mehrere Anwendungen zum benutzerdefinierten App-Profil für dieses Kundenunternehmen hinzuzufügen.
4. Klicken Sie auf die Schaltfläche **Hinzufügen** .
5. Wählen Sie eine oder mehrere Anwendungen, die zum benutzerdefinierten App-Profil hinzugefügt werden sollen.
6. Klicken Sie auf die Schaltfläche **Apps hinzufügen** .
7. Stellen Sie den **Status** der Anwendung entweder auf `Nicht zugelassen` oder `Erforderlich`.
   - Wenn eine Anwendung `nicht zugelassen` ist, deinstalliert **Enterprise Mobility Management** diese Anwendung nicht automatisch. Der Benutzer wird dazu aufgefordert, die Deinstallation manuell vorzunehmen.
   - Wenn eine Anwendung `erforderlich` ist und es sich um eine *Store-App* handelt, sendet **Enterprise Mobility Management** eine Einladung mit einem Link zur Installation der Anwendung an den Gerätebenutzer. Wenn eine Anwendung `erforderlich` ist und es sich um eine *Unternehmens-App* handelt, so wird sie automatisch per Push-Vorgang auf das Gerät übertragen.
8. Optional können Sie eine ausgewählte Anwendung aus dem benutzerdefinierten App-Profil mithilfe der Option **Zeile löschen** löschen.
9. Klicken Sie auf **Speichern**, um die Konfiguration abzuschließen.

Voreingestellte Richtlinien (schreibgeschützt)

Kaseya hat die korrekten Einstellungen für voreingestellte Eigenschaften festgelegt. Sie müssen nicht angepasst werden. Jede Art der Richtlinie – Hoch, Mittel und Niedrig – hat etwas andere Profileinstellungen.

Voreingestellte MDM-Profile (schreibgeschützt)

Sicherheitsprofil (schreibgeschützt)

Das **Sicherheitsprofil** konfiguriert Richtlinien in Bezug auf die Erstellung von PINs auf *Gerätebene* (Passcodes). PINs werden von Benutzern verwendet, um ihre mobilen Geräte zu entsperren.

Hinweis: Android unterstützt nur die folgenden Einstellungen: Simple zulassen, PIN erzwingen, Mindestlänge, Alphanumerisch erforderlich, Max. Inaktivität und Max. gescheiterte Versuche.

- **Simple zulassen** – Bei Markierung darf der Benutzer aufeinanderfolgende oder sich wiederholende Zeichen in seinen PINs (Passcodes) verwenden. So sind zum Beispiel die Passcodes `3333` oder `DEFG` erlaubt.
- **PIN erzwingen** – Bei Markierung muss der Benutzer eine PIN (Passcode) angeben, um auf das gesamte mobile Gerät zuzugreifen. Wenn diese Option nicht markiert ist, ist keine PIN erforderlich.

> Hinweis: **Voreingestellte BYOD-Profile** *(siehe 25)* können auch eine PIN auf *Anwendungsebene* erfordern. Die beiden PINs sind unabhängig voneinander.

- **Max. gescheiterte Versuche** – Legt fest, wie viele gescheiterte Versuche zur PIN-Eingabe vorgenommen werden können, bevor das Gerät gelöscht wird. Die Standardeinstellung hängt vom Gerätehersteller ab.
- **Max. Inaktivität** – Die Wartezeit in Sekunden bis zum Sperren des Geräts, während der ein Benutzer das Gerät nicht verwendet.
- **Max. PIN-Alter in Tagen** – Die maximale Anzahl der Tage, an denen dieselbe PIN verwendet wird.
- **Min. komplexe Zeichen** – Die Mindestanzahl komplexer Zeichen, die in einer PIN erforderlich sind.
- **Mindestlänge** – Die erforderliche Mindestlänge für eine PIN.
- **Alphanumerisch erforderlich** – Bei Markierung sind sowohl Buchstaben als auch Zahlen erforderlich.
- **PIN-Historie** – Bei Markierung wird ein PIN-Verlauf aufgezeichnet.
- **Max. Aufschub** – Gibt an, wie schnell das Gerät nach der Verwendung entsperrt werden kann, ohne dass erneut die PIN eingegeben werden muss.

iOS-Profil (schreibgeschützt)

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Anwendungsinstallation zulassen** – Bei Markierung dürfen Anwendungen installiert werden.
- **Kamera zulassen** – Bei Markierung ist die Kamera des Geräts aktiviert.
- **Max. gescheiterte Versuche** – Wenn der Benutzer die Anzahl der zulässigen Versuche zur Passcode-Eingabe überschreitet, in der Regel 10, wird das Telefon gesperrt. Das Telefon kann erst wieder verwendet werden, wenn es auf Werkseinstellungen zurückgesetzt wird, wodurch alle Daten vom Gerät gelöscht werden. Nach Zurücksetzen des Telefons kann es auf das letzte vorgenommene Backup wiederhergestellt werden.
- **Screenshot zulassen** – Bei Markierung kann das Gerät Momentaufnahmen seines Bildschirm erstellen.
- **YouTube zulassen** – Bei Markierung ist YouTube aktiviert.
- **iTunes zulassen** – Bei Markierung ist iTunes aktiviert.
- **Safari zulassen** – Bei Markierung ist der Safari-Webbrowser aktiviert.
- **Face Time zulassen** – Bei Markierung können Benutzer Videoanrufe über Face Time tätigen und annehmen.
- **Automatisches Synchronisieren beim Roaming zulassen** – Bei Markierung synchronisieren sich Geräte während des Roaming. Wenn nicht markiert, werden Geräte nur dann synchronisiert, wenn ein Benutzer auf das Konto zugreift.
- **Siri zulassen** – Bei Markierung können Benutzer Siri, Sprachbefehle oder Diktat verwenden.
- **Sprachwahl zulassen** – Bei Markierung können Benutzer durch Sprachbefehle wählen.
- **In-App Purchase zulassen** – Bei Markierung können Benutzer In-App-Käufe vornehmen.
- **Eingabe des Benutzerkennworts für iTunes Store bei allen Einkäufen erzwingen** – Bei Markierung müssen Benutzer vor dem Einkaufen ihr Apple-ID-Kennwort eingeben. Normalerweise gibt es eine kurze Aufschubzeit nach einem Einkauf, bevor Benutzer sich für weitere Einkäufe erneut authentifizieren müssen.

- **Multiplayer-Spiele zulassen** – Bei Markierung können Benutzer Multiplayer-Spiele im Game Center spielen.
- **Hinzufügen von Game Center-Freunden zulassen** – Bei Markierung können Benutzer Freunde im Game Center hinzufügen.
- **Betrugswarnung erzwingen** – Bei Markierung warnt Safari Benutzer, wenn besuchte Websites als betrügerisch oder gefährlich eingestuft werden.
- **JavaScript aktivieren** – Bei Markierung führt Safari JavaScript auf Websites aus.
- **Pop-ups blockieren** – Bei Markierung ist die Pop-up-Blockierungsfunktion von Safari aktiviert.
- **Cookies zulassen** – Wählen Sie aus, wann Cookies zugelassen werden sollen: `Nie`, `Von besuchten Seiten`, `Immer`.
- **Backups zulassen** – Bei Markierung können Benutzer ihr Gerät in iCloud sichern.
- **Dokumentsynchronisierung zulassen** – Bei Markierung können Benutzer Dokumente in iCloud speichern.
- **Photo-Stream zulassen (Deaktivieren kann Datenverlust zur Folge haben)** – Bei Markierung können Benutzer Fotostream aktivieren.
- **Senden von Diagnosedaten an Apple zulassen** – Bei Markierung werden iOS-Diagnosedaten an Apple gesendet.
- **Zulassen, dass Nutzer nicht vertrauenswürdige TLS-Zertifikate akzeptiert** – Bei Markierung werden Benutzer gefragt, ob sie Zertifikaten vertrauen möchten, die nicht verifiziert werden können. Diese Einstellung gilt für Safari und E-Mail-, Kontakt- und Kalenderkonten.
- **Verschlüsselte Backups erzwingen** – Wenn nicht markiert, dann kann der Benutzer in iTunes auswählen, ob eine Sicherung vom Gerät auf einen lokalen Rechner verschlüsselt werden soll oder nicht. Bei Markierung wird der Benutzer dazu gezwungen, die Sicherung zu verschlüsseln. Wenn eine Sicherung verschlüsselt wird, wird der Benutzer durch ein Textfeld auf dem Gerät dazu aufgefordert, ein Verschlüsselungskennwort einzugeben.
- **Explizite Musik und Podcasts zulassen** – Bei Markierung werden anstößige Musik oder Videoinhalt im iTunes Store angezeigt und nicht ausgeblendet. Anstößiger Inhalt wird bei der Aufführung im iTunes Store von den Inhaltsanbietern, wie z. B. Plattenfirmen, markiert.

Voreingestellte BYOD-Richtlinien (schreibgeschützt)

Zugriffsprofil (schreibgeschützt)

- **Neue Benutzer benötigen Bestätigung vom Admin vor Verwendung des Geräts –** Wenn eine Bestätigung durch den Administrator erforderlich ist, erhält der Benutzer beim ersten Zugriffsversuch auf **Enterprise Mobility Management**die Meldung "Bestätigung ist erforderlich".
- **Benutzergerät meldet sich nach n fehlgeschlagenen Versuchen ab** – Anzahl der Versuche.

Sicherheitsprofil (schreibgeschützt)

- **Mobiler Zugriff erfordert PIN-Eingabe** – Bei Aktivierung ist ein PIN (Passcode) auf *Anwendungsebene* bei jedem Start der Anwendung erforderlich. Bei Aktivierung wird der Benutzer aufgefordert, beim ersten Zugriffsversuch auf die Anwendung einen Passcode zu erstellen.

  Hinweis: **Voreingestellte MDM-Profile** *(siehe 23)* können auch einen PIN auf *Geräteebene* erfordern. Die beiden PINs sind unabhängig voneinander.

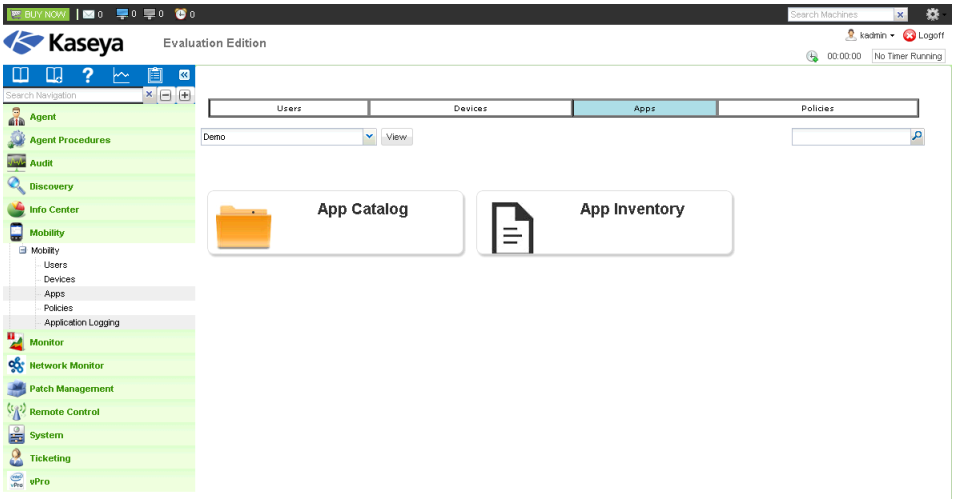
  - Nur wenn vom Benutzer aktiviert
  - Immer wenn die Anwendung aktiviert wird
  - Nach Inaktivität von N Minuten
- **Kennworteingabe für mobilen Zugriff erforderlich alle** – N Minuten, Stunden oder Tage.
- **Benutzer dürfen Elementinhalt an andere mailen** – Ja/Nein.
- **Benutzer dürfen Elementinhalt mit Nicht-Suite-Anwendungen öffnen** – Ja/Nein.

- **Benutzer dürfen Bilder in der Fotogalerie des Geräts speichern** – Ja/Nein.
- **Benutzer dürfen Nicht-Suite-Inhalt drucken** – Ja/Nein.
- **Benutzer dürfen in Nicht-Suite-Apps kopieren/einfügen** – Ja/Nein. Falls nein, wird eine `paste blocked by policy` Meldung angezeigt, wenn ein Benutzer versucht, von einer sicheren Container-Anwendung in eine externe Anwendung zu kopieren. Das Kopieren von einer externen Anwendung in eine sichere Container-Anwendung ist niemals blockiert.

Verwalten von Anwendungen auf Geräten

Enterprise Mobility Management kann entweder ausgewählte Anwendungen auf mobilen Geräten erfordern oder nicht zulassen. Dazu gehören sowohl Anwendungen, die aus App-Stores heruntergeladen wurden, als auch proprietäre *Unternehmens-Apps*.

1. Navigieren Sie zur Seite **Anwendungen**.
2. Wählen Sie ein Kundenunternehmen.



3. Sie können eine der zwei Optionen auswählen:
   - Die Seite **App-Katalog** *(siehe 26)* enthält einen Katalog der *App-Elemente*. Ein App-Element ist ein Datensatz, der eine einzelne Anwendung eindeutig identifiziert, welche auf einem mobilen Gerät erforderlich bzw. nicht zugelassen ist.

     Hinweis: Eine Anwendung muss zum **App-Katalog** hinzugefügt werden, bevor sie in ein Anwendungsprofil für ein bestimmtes Kundenunternehmen eingeschlossen werden kann.

   - Die Seite **App-Bestand** erzeugt eine Liste von Kandidaten für App-Elemente basierend auf einem Audit aller von **Enterprise Mobility Management** verwalteten mobilen Geräten. Nutzen Sie die Liste, um das Format der App-Datensätze zu bestimmen, die Sie zum **App-Katalog** hinzufügen möchten.
4. Klicken Sie für diese Beta-Version auf den **App-Katalog**. Die Konfiguration der Anwendungen auf verwalteten Geräten erfolgt in zwei Schritten:
   - **Konfigurieren des App-Katalogs** *(siehe 26)*.
   - **Konfigurieren der App-Profile in einer Richtlinie** *(siehe 23)*.

Konfigurieren des App-Katalogs

Der **App-Katalog** enthält einen Katalog der App-Elemente. Jedes App-Element identifiziert eindeutig

eine einzelne Anwendung, welche auf einem mobilen Gerät erforderlich bzw. nicht zugelassen ist. Nach dem Hinzufügen zum Katalog können App-Elemente dann zu den **App-Profilen** *(siehe 23)* einer Richtlinie hinzugefügt werden, die einem Kundenunternehmen zugeordnet ist.

Hinweis: Für jedes Kundenunternehmen wird ein individueller **App-Katalog** geführt.

Hinzufügen eines neuen App-Elements

1. Wählen Sie bei Bedarf das richtige Kundenunternehmen aus.
2. Klicken Sie auf **Neu**. Der ausgewählte *App-Typ* gibt an, ob die Anwendung von einem App-Store installiert oder von VSA als Unternehmens-App heruntergeladen wird.
   - **Store-App** – Bei Auswahl muss eine **URL** angegeben werden.
   - **Unternehmens-App** – Bei Auswahl muss eine **App-Programmdatei** hochgeladen werden.
3. Wenn Sie eine **Store-App** auswählen, wird der Dialog **Neue Store-App** angezeigt.
   - Wählen Sie das Optionsfeld **Android** oder **iOS**.
   - Geben Sie optional einen Suchbegriff ein, um die Liste der ausgegebenen Anwendungen aus dem ausgewählten Store zu filtern.
   - Wählen Sie eine Anwendung in der Liste aus.
   - Klicken Sie entweder auf die Schaltfläche **Hinzufügen** oder **Hinzufügen & Neu**.

   Ihre Anwendung wurde zum **App-Katalog** hinzugefügt.
4. Wenn Sie eine **Unternehmens-App** auswählen, wird der Dialog **Neue Unternehmens-App** angezeigt.
   - Wählen Sie das Optionsfeld **Android** oder **iOS**.
   - Geben Sie einen **Namen** für die Anwendung im **App-Katalog** ein.
   - Navigieren Sie zum **Paket**, das in VSA hochgeladen werden soll. Das **Paket** ist entweder eine Android `.apk`-Datei oder eine iOS `.ipa`-Datei.
   - Klicken Sie entweder auf die Schaltfläche **Hinzufügen** oder **Hinzufügen & Neu**.

   Ihre Anwendung wurde zum **App-Katalog** hinzugefügt.

Arbeiten mit vorhandenen App-Elementen

Im Menü **Aktionen** sind die folgenden Optionen für im **App-Katalog** vorhandene Anwendungen verfügbar.

- **Bearbeiten** – Bearbeitet ein ausgewähltes App-Element im **App-Katalog**.
- **Löschen** – Löscht ein ausgewähltes App-Element aus dem **App-Katalog**.
- **Einladen** – Sendet eine Meldung an einen oder mehrere Benutzer, um sie zur Installation ausgewählter Anwendungen auf ihre mobilen Geräten einzuladen.

Anzeigen des App-Bestands

`Enterprise Mobility Management > Apps > App-Bestand`

Die Seite **App-Bestand** erzeugt für das ausgewählte Kundenunternehmen und Richtlinienprofil eine Liste von App-Elementen anhand der Anwendungen, die auf den verwalteten mobilen Geräten ermittelt wurden. Nutzen Sie die Liste, um das Format der App-Datensätze zu bestimmen, die Sie zum **App-Katalog** *(siehe 26)* hinzufügen möchten.

Tabellenspalten

- **OS** – `Android` oder `iOS`.
- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.
- **Version** – Die Versionsnummer der Anwendung. Beispiel: `1.2.0.0`.

WorkBrowser und WorkDocs

Enterprise Mobility Management bietet Benutzern von mobilen Geräten sicheren Zugriff auf die internen Websites und Dokumente ihres Unternehmens mithilfe von zwei Container-Apps.

- **WorkBrowser** *(siehe 28)* – Bietet sicheren Zugriff auf interne Websites.
- **WorkDocs** *(siehe 28)* – Ermöglicht das sichere Anzeigen und Bearbeiten von Dokumenten in internen Netzwerken oder lokal Speichern auf mobilen Geräten.

Verwendung von WorkBrowser

Der **WorkBrowser** ist ideal für Personen, die mobil sind und Verbindung mit dem Office halten müssen. **WorkBrowser** bietet, bei Ausführung und im Ruhezustand, einen sicheren Zugriff auf interne Intranets, Dateien und Verzeichnisse. Ausgewählte Dateien können unter Verwendung von **WorkDocs** *(siehe 28)* bearbeitet werden.

Herunterladen von WorkBrowser

- Apple-Geräte – Herunterladen mit dem in Ihrer E-Mail-Einladung angegebenen Link.
- **Android-Geräte** *(https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workbrowser)* – Herunterladen mit dem in Ihrer E-Mail-Einladung angegebenen Link.

Anforderungen für verwaltete mobile Geräte

- IOS-Version (7.0 und höher)
- Android-Version 4.0.3 und höher

Passcodes

Sie werden eventuell aufgefordert, ein Pin (Passcode) auf *Anwendungsebene* zu erstellen, um **WorkBrowser** zu verwenden. Danach müssen Sie diese PIN bei jedem Zugriff auf die **WorkBrowser**-Anwendung eingeben.

Sites

Die **Sites**-Liste zeigt alle Websites an, auf die Sie über **Enterprise Mobility Management** Zugriff haben.

Anzeigen und Bearbeiten von Dateien

Beim Browsen von Webseiten in **WorkBrowser** können Sie Dateien anzeigen. Angezeigte Dateien können unter Verwendung von **WorkDocs** *(siehe 28)* bearbeitet werden.

Verwenden von WorkDocs

Mit WorkDocs können Sie Dokumente anzeigen oder bearbeiten, die in einem internen Netzwerk oder lokal im **Sicherheitsspeicher** auf Ihrem mobilen Gerät gespeichert sind. Sie können Dokumente zudem verschieben, kopieren oder löschen. Lokal gespeicherte Dokumente werden verschlüsselt und bleiben vom Rest der Umgebung auf dem mobilen Gerät isoliert.

Herunterladen von WorkDocs

- Apple-Geräte – Herunterladen mit dem in Ihrer E-Mail-Einladung angegebenen Link.
- **Android-Geräte**
  https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workdocs – Herunterladen mit dem in Ihrer E-Mail-Einladung angegebenen Link.

Anforderungen für verwaltete mobile Geräte

- IOS-Version *(7.0 und höher)*
- Android-Version 4.0.3 und höher

Passcodes

Sie werden eventuell aufgefordert, eine PIN (Passcode) auf *Anwendungsebene* zu erstellen, um **WorkDocs** zu verwenden. Danach müssen Sie diese PIN bei jedem Zugriff auf die **WorkDocs**-Anwendung eingeben.

Sites

Die **Sites**-Liste zeigt alle **WorkDocs**-Websites an, auf die Sie via **Enterprise Mobility Management** Zugriff haben. Jede **WorkDocs**-Site bietet Zugriff auf eine Navigationsstruktur von Ordnern und Dokumenten. *Diese Dokumente werden nicht auf Ihrem Gerät gespeichert, es sei denn, sie befinden sich im* **Sicherheitsspeicher***.*

Sicherheitsspeicher

Die **WorkDocs**-Site zeigt zudem einen **Sicherheitsspeicher**ordner mit lokalen Dokumenten an, die auf Ihrem Gerät gespeichert sind. Derselbe **Sicherheitsspeicher**ordner wird auf allen **WorkDocs**-Sites, auf die Sie Zugriff haben, freigegeben.

Autorisierung

Je nachdem, welche Art von Autorisierung dem Dokument zugewiesen ist, werden Sie eventuell aufgefordert, Anmeldedaten einzugeben.

Bearbeiten von Dokumenten

Durch Auswählen einer Datei können Sie eine Vorschau der Datei anzeigen. Wählen Sie die Schaltfläche **Bearbeiten** über der in der Vorschau angezeigten Datei, um den Datei-Editor zu starten.

Beim ersten Laden des Editors können Sie das **Datei**symbol auswählen und die Option **Speichern unter** verwenden, um die aktuelle Datei unter einem neuen Namen und/oder Speicherort zu speichern. Sobald Sie beginnen, Änderungen vorzunehmen, kann das **Datei**symbol verwendet werden, um die aktuelle Datei unter demselben Namen und Speicherort der Originaldatei zu speichern. Wenn eine Sicherung fehlschlägt, sollten Sie sich vergewissern, dass Sie Schreibzugriff auf den Speicherort des Dokuments haben.

Verschieben, Kopieren und Löschen von Dateien

Sie können Dateien von jedem Ort aus verschieben, kopieren oder löschen.

- Wählen Sie **Bearbeiten** über der Quelldateiliste des Dokuments, um diese Optionen anzuzeigen.
- Wählen Sie die Datei(en) aus, die Sie verschieben, kopieren oder löschen möchten.
- Für die Aktionen **Kopieren** und **Verschieben** werden Sie aufgefordert, den Namen und den Speicherort der neuen Datei anzugeben. Um eine lokale Kopie der Datei zu speichern, kopieren oder verschieben Sie diese in Ihren **Sicherheitsspeicher**.
- Um eine Datei zu löschen, wählen Sie die Schaltfläche **Löschen**. Sie werden aufgefordert, die Löschvorgänge der Datei zu bestätigen.

Favoriten

Jeder beliebige Ordner unter dem Stammverzeichnis kann als **Favorit** gespeichert werden. Um einen Ordner als **Favorit** zu speichern, wählen Sie das "Stern"-Symbol unten in der Dateiliste. Das "Stern"-Symbol verdunkelt sich, um anzuzeigen, dass dieser Ordner nun ein **Favorit** ist.

Ordner, die als **Favorit** gekennzeichnet sind, werden zusammen mit Ihren Dokumentquellen angezeigt. Durch die Auswahl von **Favorit** wird eine Verknüpfung hergestellt, um direkt zu diesem Speicherort zu gelangen.

Protokollierung der Modulaktivität

Sie können die Anwendungsaktivität im **Mobility**-Modul über die Seite **Anwendungsprotokolle** überprüfen. Wenn Informationen unerwartet geändert oder entfernt wurden, prüfen Sie diese Seite, um zu ermitteln, welche Ereignisse und Administratoren möglicherweise beteiligt waren.

Zu den Einträgen zählen:

- **Ereignis-ID**
- **Ereignisname**
- **Meldung**
- **Admin**
- **Ereignisdatum**

Protokollierte Ereignisse umfassen Folgendes:

Passcode löschen
Gerät erstellt
Gerät gelöscht
Gerät gefunden
Einladung erneut gesendet
Gerät sperren
Verlorenes Gerät
Befehle als abgeschlossen kennzeichnen
Benachrichtigung bearbeiten
Check-in anfordern
Protokolle anfordern
Audit starten
Geplanter Audit
Alarm auf Gerät auslösen
Geräteverfolgung starten
Geräteverfolgung anhalten
Gerät aktualisiert
Gerät löschen

Inhaltsverzeichnis

A

Anzeigen des App-Bestands • 27
Audit-Aktionen • 14

B

Befehlsstatus • 13
Benachrichtigungsaktionen • 15
Benutzerdef. Anwendungsrichtlinien • 23
Benutzerdefinierte BYOD-Profile • 21
Benutzerdefinierte MDM-Richtlinien • 19
Benutzeroberfläche • 3

E

Enterprise Mobility Management
Modulvoraussetzungen • 2

G

Geräteaktionen • 15
Gerätedetails anzeigen • 15

K

Konfigurieren der Active Directory Integration • 4
Konfigurieren des App-Katalogs • 26
Konfigurieren eines E-Mail-Profils • 20
Konfigurieren eines Web Clip-Profils • 19
Konfigurieren eines WiFi-Profils • 20

M

Messaging-Aktionen • 14

N

Nachverfolgungsaktionen • 14

O

Onboarding von Benutzern • 11
Onboarding-Kunden • 8

P

Protokollierung der Modulaktivität • 30

R

Regeln konfigurieren • 18

U

Überblick • 1

V

Verloren/Gefunden-Aktionen • 14
Verwalten von Anwendungen auf Geräten • 26
Verwalten von Geräten • 12
Verwenden von WorkDocs • 28
Verwendung von WorkBrowser • 28
Voreingestellte BYOD-Richtlinien (schreibgeschützt) • 25
Voreingestellte MDM-Profile (schreibgeschützt) • 23
Voreingestellte Richtlinien (schreibgeschützt) • 23

W

WorkBrowser und WorkDocs • 28